Cybercrime and its impact on extraditions in the Republic of South Africa

by

Pravina Harichander Rughoonandan

Student number: 8360189

submitted in accordance with the requirements
for the degree of

MASTER OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

Study Supervisor: Dr B.J. Gordon

(September 2021)

DECLARATION

Name: Pravina Harichander Rughoonandan

Student number: 8360189

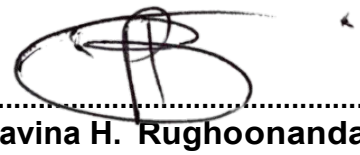
Degree: Master of Laws (LLM)

Title: **'Cybercrime and its impact on extradition in the Republic of South Africa'**

I declare that the above dissertation is my work and that all sources I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to an originality checking software and it falls within the accepted originality requirements.

I further declare that I have not previously submitted this work, or part of it for examination at UNISA for another qualification or at any other higher education institution.



2021/12/17

....

Pravina H. Rughoonandan **Date**

ACKNOWLEDGEMENT

My sincere gratitude thanks to my supervisor, Dr B.J. Gordon, for guiding and assisting me in this arduous journey that has taught me to be patient and persevere.

Many thanks to the facilitators of the M&D Postgraduate Support Programme for their passion and commitment to student excellence.

All authors and sources cited in this study are duly acknowledged and appreciated for their scholarly contributions.

I wish to further express my gratitude and a personal note of thanks to Mrs Doepie de Jongh.

I am indebted to my son for the technical support, and trust that he will complete his Master's degree soon.

A special 'thank you' to my brother Neesham, for all the unconditional love and support. I could not have accomplished this feat without him. He is my rock and inspiration. This thesis is for you brother, with all my love.

ABSTRACT

This study explores several South African cyber laws by comparing them to international precepts of the UK and the US, and determines how they impact on extraditions. The extradition process is largely governed by the dual criminality principle and compliance with the international obligations before a person can be extradited, irrespective of the existence of a treaty. South Africa has acceded to some conventions, but not with others, which decelerates the process of achieving global harmonisation in e-crime. The constant evolvement and capricious nature of cyber infractions may impede the securing of critical data expeditiously due to lack of adroitness and proficiency in law enforcement agencies. The Cybercrimes Bill recently signed into law, on 26 May 202, has been hailed, but criticism renders the pragmatic effect disappointing in the curtailment of online freedom and the perilous criminalisation of false communication. Online crime scenes are not territorially bound and control over cyberspace may be problematic in the absence of global harnessing of cybercrime for an extradition to be workable.

KEY TERMS

Cybercrimes

Cybercrimes Bill

Cyberspace

Double Criminality Principle

Extraditions

Mutual Legal Assistance

Treaties

United Kingdom

South Africa

United States

ABBREVIATIONS

ACPO	Association of Chief Police Officers
AU	African Union
AJIC	The African Journal of Information and Communication
CFAA	Computer Fraud and Abuse Act
ConCourt	Constitutional Court
CMA	Computer Misuse Act
CPA	Criminal Procedure Act
CSA	Correctional Services Act
DNA	Deoxyribonucleic acid
DPA	Data Protection Act
EAW	European Arrest Warrant
ECTA	Electronic Communications and Transactions Act
EU	European Union
EU GDPR	EU General Data Protection Regulation
FA	Fraud Act
FCA	Financial Conduct Authority
FICA	Financial Intelligence Centre Act
GDPR	General Data Protection Regulation
GG	Government Gazette
ICCM	International Co-Operation in Criminal Matters
ICCMA	International Co-Operation in Criminal Matters Act
IP	Internet Protocol
IPA	Investigatory Powers Act
LEA	Law Enforcement Agency
LJIL	Leiden Journal of International Law
MLA	Mutual Legal Assistance
Monash ULR	Monash University Law Review
NACDL	National Association of Criminal Defence Lawyers
NCA	National Crime Agency
NCOP	National Council of Provinces
NCPF	National Cybersecurity Policy Framework
NCSC	National Cybersecurity Centre
NIIPA	National Information and Infrastructure Protection Act

NISR	Network and Information Systems Regulations
NPAA	National Prosecuting Authority Act
OECD	Organisation for Economic Co-operation and Development
PELJ	Potchefstroom Electronic Law Journal
POCA	Proceeds of Crime Act
POPIA	Protection of Personal Information Act
R2K	Right2Know
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
RSA	Republic of South Africa
SA Crim Q	South African Crime Quarterly
SAJHR	South African Journal on Human Rights
SAPS	South African Police Service
SAPSA	South African Police Service Act
SCA	Supreme Court of Appeal
T-CY	Cybercrime Convention Committee
UK	United Kingdom
UK IPA 2016	United Kingdom Investigatory Powers Act 2016
UN	United Nations
USA	United States of America

Contents

Chapter 1: Introduction

1.1 Background

The exigency for operative transnational and international criminal justice ought to be carefully balanced with the imperative for State integrity and territorial sovereignty.[1] Malefactors have progressively become involved in cyber activities, creating new criminal and procedural law challenges in cybercrimes[2] with the inadvertent but consequential impact it has on extraditions in South Africa. The Convention on Cybercrime is the incipient international treaty designed to thwart Internet and computer crime (cybercrime).[3] In this regard, South Africa's cybersecurity legislation lags behind that of advanced economies.[4] The first statutory provision on cybercrime[5] was created in Chapter XIII of the Electronic Communications Transactions Act 25 of 2002. The new Cybercrimes Act 19 of 2020 will be fully operational by proclamation in the Gazette.[6] The paltry cybersecurity laws not only have an impact on extradition concerning application of the double criminality principle, but also deviate from the legal precepts and core principle of the rule of law, that all persons and authorities be entitled to, and bound by the benefit of laws publicly and prospectively so promulgated.[7] The effect is that an extradition premised on cyber infractions would be unlawful if the correct procedures were not followed.[8]

The consequences of cyber freedom in South Africa are proving to be costly, not only with the delays in the enactment of legislation and proclamation, but

---

1 Murdoch Watney, 'A South African perspective on mutual legal assistance and extradition in a globalized world' (2012) 15 PELJ 293.

2 Vinesh Basdeo, 'Criminal and Procedural Legal Challenges of Identity Theft in the Cyber and Information Age' (2017) 30 SAJCJ 363.

3 Convention on Cybercrime - Treaty 185 <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm> accessed 22 April 2020.

4 Ewan Sutherland, 'Governance of Cybersecurity - The case of South Africa' (2017) 20 AJIC 83-112.

5 ECT Act, ss 85-89.

6 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read' (2021) <https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa> accessed 2 June 2021.

7 Tom Bingham, *The rule of law* Part 1 (Penguin 2011) 8.

8 *Mackeson v Minister of Information, Immigration and Tourism* 1980 (1) SA 747 (ZR) at 753-7.

also monetarily, with billions of Rands lost due to cybercrime.[9] Imperious fugitives from justice enjoy freedom of movement without fear of being arrested[10] or extradited. South Africa's cyber laws and international edicts form the linchpin for cyber extraditions and global harmonisation.

Accordingly, the research focuses on extradition and dual criminality, South Africa's cyber legislation, as well as the legal philosophy of the United Kingdom (UK) and the United States (US). For many years, the latter two countries' legal systems and their characterisation by judicial precedence, were regarded as the epitome of the common law system.[11] The US is viewed as profoundly exemplary in applying extant criminal law pertinent to cybercrime regulation, with efforts made since the 1970's.[12] The UK, on the other hand, has expanded the domain of common law fraud by enacting the Computer Misuse Act of 1990 in order to adapt to the digital world and its attendant cyber infractions.

1.2 Statement of the problem

In law, the double criminality principle requires that an individual's extradition should be confirmed and preceded by the criminality of such conduct in the country where the perpetrator is situated, as well as the country where the person will stand trial. Where cybercrime legislation is deficient in either of these countries, extradition will fail. This study deals with the problem by examining the interplay between cybercrime, legislation, extradition and the double criminality principle, with particular focus on the effect of cybercrime on extradition.

1.2.1 The problem arises with the world-wide commission of cybercrimes. It is always going to be difficult to determine the locus *commissi delicti* (the place at which the offences were allegedly committed),[13] and deciding

---

9 YarikTurianskyi 'Balancing Cyber-Security and Internet Freedom in Africa' *Africa Portal* (31 January 2018) <https://media.africaportal.org/documents/OP_275_GAP_Turianskyi_FINAL_WEB.pdf> accessed 6 June 2020.

10 Jamil Ddamulira Mujuzi, 'The South African International Co-Operation in Criminal Matters Act and the issue of evidence' (2015) 48 De Jure 351.

11 Qianyun Wang, *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe* (Wolf Legal 2016) 27.

12 Wang, *A Comparative Study of Cybercrime in Criminal Law* 99.

13 See Stephen Jeffries and Edward Apeh, 'Standard operating procedures for cybercrime investigations: a systematic literature review' in Vladlena Benson and John McAlaney,

who commands overarching finality in any investigation, prosecution and extradition of a South African cybercrime.

1.2.2 At present, the problem is that the South African cybercrime legal framework comprises a hybrid of the common law and different pieces of legislation.[14] Cybercrime infractions are largely regulated by the Electronic Communications and Transactions Act 25 of 2002 (hereinafter ECT Act), which is not at par with international standards and the dynamism of technology.[15] However, this is a wide piece of legislation,[16] and only Chapter Eight of the ECT Act, which became law in 2002, deals with cybercrimes with the penalty clauses referred to in section 89 of the self-same Act.[17]

1.2.3 The Cybercrimes Act 19 of 2020, previously the Cybercrimes Bill [B6 of 2017], is partly in operation. The Act consolidates and codifies several existing infractions of cybercrime and creates new kinds of offences that are not present in South African law.[18] The Act delves on penalties[19] for these cybercrime offences and allocates investigation, search, access and seizure powers[20] relevant to prosecution of such infractions and regulates jurisdiction[21] of the courts and wider sentences. The

---

Emerging Cyber Threats and Cognitive Vulnerabilities (Academic Press 2020) where they refer to Brenner, Lee, Cox and Siber, (2006) 145-162 156.

14 Cliffe Dekker Hofmeyr Inc, 'The International Comparative Legal Guide to: Cybersecurity' (2nd edn 2019) Chapter 29 185-191 <https://www.mhmjapan.com/content/files/00032671/The%20International%20Comparative%20Legal%20Guide%20to%20Cybersecurity%202019%20-%20Japan%20Chapter.pdf> accessed 20 March 2020.

15 Cliffe Dekker Hofmeyr Inc, 'The International Comparative Legal Guide'.

16 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read'.

17 Act 25 of 2002.

18 Cliffe Dekker Hofmeyr Inc, 'The International Comparative Legal Guide'.

19 Cybercrimes Act 19 of 2020, ss 14 and 22.

20 Cybercrimes Act 19 of 2020, ss 24-43, ch 5.

21 Cybercrimes Bill [B6 of 2017], s 23.

Cybercrimes Bill[22] was even criticised for curtailing freedom of expression.[23]

1.2.4 Section 32 of the Constitution[24] upholds everyone's right of access to any information held by the State or held by another person for the protection of any rights. In order to give effect to section 32, the Promotion of Access to Information Act (PAIA) was enacted in 2000, but does not have provisions that are sufficient for data protection, as PAIA was not intended for that purpose and is not data protection legislation.[25] Finally, on 1 July 2020, certain sections of Protection of Personal Information Act 4 of 2013 (POPI) came into effect and the rest was on 1 July 2021.[26] POPI imposes administrative fines and punitive measures for infringement of its provisions[27] however, the question is whether the POPI Act fulfils the quintessential international standards of the right to privacy.[28]

1.3 Research question

1.3.1 Main research question

Does exiguous cybercrime legislation impact on extradition, especially in the context of the legal prescripts for an extradition?

---

22 B6 of 2017.

23 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill' (8 April 2017) <https://www.R2k.Org.Za/2017/08/11/R2k-Submission-on-the-Cybercrimes-Bill-2017> accessed 23 December 2020.

24 Constitution of the Republic of South Africa, 1996, s 32 provides:
'(1) Everyone has the right of access to -
(*a*) any information held by the state; and
(*b*) any information that is held by another person and that is required for the exercise or protection of any rights.
(2) National legislation must be enacted to give effect to this right and may provide for reasonable measures to alleviate the administrative and financial burden on the state.'

25 L Johannessen, J Klaaren and J White, 'A motivation for legislation on access to information' (1995) 112 SALJ 56-57. Typically, data protection legislation performs three functions: it prevents unauthorized disclosure and use of private information; it allows for the correction of personal information held by another, for example the United Kingdom Data Protection Act 1984 and the Canadian Privacy Act 1985.

26 Cyril Ramaphosa, 'Commencement of certain sections of the Protection of Personal Information Act, 2013' (22 June 2020) <http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013> accessed 22 June 2020 enforcement of the POPI Act is now in effect, after facing huge implementation challenges.

27 Cliffe Dekker Hofmeyr Inc, 'The International Comparative Legal Guide'.

28 POPI Act 4 of 2013, Preamble.

1.3.2 Sub-questions

i. What does South African law on extraditions encompass?
ii. Seeing that extradition requires double criminality, would this requirement be more difficult to satisfy in relation to cybercrime laws in South Africa?
iii. How do the United Kingdom and United States address cybercrime laws?
iv. Does the application of the rule of law mean that cyber criminals cannot be extradited where cybercrime legislation is exiguous, and is there an obligation to prosecute where there is no extradition?
v. How can a mutual assistance request be sought in order to secure evidence, and is mutual legal assistance effective?

1.4 Scope of the study

The study is founded on both the conceptual and substantive assumptions that defined the problem statement and the main research question. These assumptions are:

1.4.1 South Africa's extraditions are governed by the Extradition Act.[29] The nub of an extradition is the principle of double criminality, which demands the nature of the conduct to be an extraditable infraction and constitute a crime in both states.[30] Extradition law and praxis also subsume international law on the level of the judicial and executive branches of government.[31] South Africa consented to the multilateral European Convention on Extradition of 1957, thereby becoming party to an extradition agreement with many other States.[32] The international commitment is amiable, creating the expectation that obligations will be continuous, and should not bring about disquietude.

1.4.2 The literature germane to cyber legislation in South Africa, United Kingdom (UK) and United States (US) is appraised. The UK and the US

---

29 Extradition Act 67 of 1962.
30 John Dugard, Max du Plessis and Anton Katz, *International Law: A South African Perspective* (Juta 2012) 219.
31 Anton Katz, 'The incorporation of extradition agreements' (2003) 16 SACJ 311-322.
32 Council of Europe 'European Convention on Extradition' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/024/signatures?p_auth=fYhfKTof> accessed 20 July 2020.

are likened to cybercrime primogenitors, with the Cybercrime Convention of 2001,[33] the European Convention on Mutual Assistance in Criminal Matters of 1959,[34] as well as the first US Computer Fraud and Abuse Act of 1984[35] and its consequent expansions over the years. In the UK, the Computer Misuse Act 1990[36] was promulgated but considered insufficient as it largely addressed hacking crimes.[37] Meanwhile, the Fraud Act of 2006 – effectively applied in 2007 - was enacted to address e-crimes together with the Police and Justice Act of 2006. Laws must be dialectical and codified for worldwide harmonisation in dealing with the scourges of e-crime, with no exception or reason for South Africa's non-conformity. Accordingly, the new Cybercrime Act 19 of 2020 must effectively deal with cybercrime infractions.

1.4.3 The immanent delays and anomalies in enactment of legislation or implementation give rise to the issue of prescription of offences in an extradition request. Furthermore, the absence of a treaty may require a state to surrender or punish the wrongdoer under its own laws,[38] while the nationality exception shifted a lot of attention to the *aut dedere aut*

---

33 'Explanatory Report to the Convention on Cybercrime (European Treaty Series No 185)' <https://rm.coe.int/16800cce5b> accessed 4 May 2020.

34 European Convention on Mutual Assistance in Criminal Matters 'European Treaty Series – No 30' <https://rm.coe.int/16800656ce> accessed 14 January 2021.

35 Computer Fraud and Abuse Act 1984, Coded as 18 U.S.C. § 1030, which is changed into the Computer Fraud and Abuse Act in 1986.

36 This creates three distinct criminal offenses: Unauthorized access to computers, including the illicit copying of software held in any computer. This carries a penalty of up to six months' imprisonment or up to a £5000 fine and will be dealt with by a magistrate. This covers hobby hacking and, potentially, penetration testing. Unauthorized access with intent to commit or facilitate commission of further offenses (such as fraud or theft), which covers more serious cases of hacking with a criminal intent. This has a penalty of up to five years' imprisonment and an unlimited fine. Because it is a serious offense, it will be a trial by jury (12 jolly good people).
Unauthorized modification of computer material, which includes the intentional and unauthorized destruction of software or data; the circulation of 'infected' materials online ('viruses'); and the unauthorized addition of a password to a data file ('crypto viruses'). This offense also carries a penalty of up to five years' imprisonment and an unlimited fine. It is also a serious offense, so it too will be a trial by jury.

37 Hamid Jahankhani and Amin Hosseinian-far, 'Cybercrime classification and characteristics' in B Akhgar, A Staniforth and F Bosco (eds), *CyberCrime and Cyber Terrorism Investigator's Handbook* (Syngress 2014) 149-164.

38 Watney, 'A South African perspective on mutual legal assistance' 298.

judicare principle.[39] Therefore, the law ought to prosecute or effect an expeditious extradition, lest it renders an extradition futile and ineffective.

1.4.4 Law enforcement authorities increasingly and invariably require electronically obtained evidence provided by other countries in certain investigations. As such, evidence should be obtained efficaciously, tandem with data protection requirements and the rule of law. There should also be more efficient mutual international collaboration to adapt procedures and rules for the securance of volatile electronic evidence expeditiously.[40]

1.4.5 The limitations of the study are subject to the below-cited variables:

1.4.5.1 The date and proclamation of the Cybercrime Act 19 of 2020, unlike the POPI Act which had huge implementation problems.[41]

1.4.5.2 The Cybercrime Act is not in operation as yet and affects operations of society[42] both locally and internationally.

1.4.5.3 The non-ratification of treaties due to factors that may be political or unclear.[43]

1.5 Literature review

The research process was initiated by probing previous studies in order to explore the research field, enrich the aim of the study and to justify the nature of the research question.[44] The focal point is contingent on what was researched

---

39 Watney, 'A South African perspective on mutual legal assistance' 298.

40 Council of Europe, Conference organised under the project 'Cybercrime@Octopus' followed the decision taken in December 2013 by the Cybercrime Committee (Strasbourg June 19 and 20, 2014) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/3021_Art15Conf_Agenda_v8.pdf> accessed 8 June 2020.

41 Ramaphosa, 'Commencement of certain sections of the Protection of Personal Information Act, 2013' enforcement of the POPI Act is now in effect, after facing huge implementation challenges.

42 Stating the Obvious: Writing Assumptions, Limitations, and Delimitations <https://www.phdstudent.com/thesis-and-dissertation-survival/research-design/stating-the-obvious-writing-assumptions-limitations-and-delimitations/> accessed 5 Sept 2020.

43 Ray William London, 'Comparative data protection and security law: A critical evaluation of legal standards' (PhD thesis, University of South Africa 2013).

44 Hannah Snyder, 'Literature review as a research methodology: An overview and guidelines' (2019) 104 Journal of Business Research 333-339 334.

previously and discovered[45] in the realm of cybercrime in South Africa and its international repercussions, with specific reference to extraditions. Amongst others, the appraisal of the literature enhanced gap identification in the research subject[46] by comparing other Jurisprudences in cybercrime with South African laws and subsequently exploring the collective evidence.[47]

The theoretical framework emanates from the reviewed literature, and provides the foundational tenets of the conceptual model in order to achieve the aims of mapping and developing this research.[48] The collation of data regarding the extradition laws of South Africa and the UK, and some of the cyber laws of the UK and the US premises on identifying and understanding all potentially relevant research or processes that could have implications for this topic.[49] The obtained data is helpful in synthesizing concepts and findings from multitudinous sources to facilitate answers pertinent to the research question.

The reviewed literature is instrumental in providing acumen insights on complex areas of law and digital evidence, together with trans-border crimes and jurisdiction. Moreover, the self-same reviewed literature is a transparent strategy that enables readers' assessment of the reasonableness or otherwise of conclusions and recommendations in relation to the topic and its methodological orientation.[50] The qualitative approach has been used to identify, synthesize and analyse data concerning the state of knowledge, and to create an appropriate agendum for further studies[51] when approaching foreign jurisdictions in e-crime.

A brief overview of the legal literature attained was obtainable from a variety of sources, namely: legislation, treaties and conventions, case law, books, reports, legal journal articles and Internet resources. These were considered to be most apposite, bearing in mind the feasibility of the study, its impact on the research

---

45 Snyder, 'Literature review as a research methodology' 334.
46 Snyder, 'Literature review as a research methodology' 334.
47 Snyder, 'Literature review as a research methodology' 334.
48 Snyder, 'Literature review as a research methodology' 334.
49 Snyder, 'Literature review as a research methodology' 335.
50 Snyder, 'Literature review as a research methodology' 335.
51 Snyder, 'Literature review as a research methodology' 335.

community, as well as both the author's and reader's interest.[52] The data abstracted was mostly in the form of the effects, findings and conceptualisation of some ideas,[53] for example: the European Arrest Warrant instead of the conventional process of extradition. Data abstraction was undertaken purposefully in association with relevant research[54] on the impact of cybercrimes on extraditions. It was, therefore, necessary that the literature review method should entail identification, synthesis, and analysis of critical issues,[55] starting with extradition and cyber laws of South Africa, the UK and the US by using relevant legal sources to ensure quality and reliability.[56] The latter orientation is appropriate, as each source is used in support of arguments, comparisons and conclusions. The main study does significantly list relevant and properly referenced sources.

1.6 Research methodology

The research methodology entails a predominantly qualitative approach informed by a protracted literature study involving both primary and secondary information sources, such as: legislation and case law, academic books from reputable libraries, published and unpublished dissertations and theses, Internet sources; as well as research papers and articles in accredited legal journals.

The research focus is on the UK and the US legislations, and comparing those with South African legislation for the purpose of illustrating the latter's slow developments in keeping abreast of international law and the impact this has on extraditions. The research will explore the extradition loopholes and the difficulties attendant to the principle of reciprocity. Additionally, the research aims to bridge gaps in the extradition process regarding cybercrimes and analyse perceptions of South Africa as safely accommodating fugitives from justice.

---

52 Snyder, 'Literature review as a research methodology' 336.
53 Snyder, 'Literature review as a research methodology' 337.
54 Snyder, 'Literature review as a research methodology' 337.
55 Snyder, 'Literature review as a research methodology' 337.
56 Snyder, 'Literature review as a research methodology' 337.

1.7 Framework

The structure of the dissertation is specific to the topic, with the focal point of each chapter addressing topics that underscore and answer the research question.

Chapter 1 is a synopsis of the study and research process, and incorporates the structure and framework of the dissertation. This chapter further entails an overview of the problem statement, main research question, scope of the study and the delimitation of the chosen topic. The literature review abstracted from legal resources aims at depth and rigour, value; as well as expected contributions and solutions[57] to address the research problem, commencing with extradition law and the dual criminality principle.

Chapter 2 addresses extraditions, the double criminality principle, and the development of South Africa's case law with respect to the double criminality principle.

Chapter 3 addresses South Africa's cyber laws, including the Protection of Personal Information Act and the Cybercrimes Act and its criticisms.

Chapter 4 explores the cyber laws of the UK and the US, as well as the European Arrest Warrant.[58] Accordingly, the chapter analyses some of UK's pieces of legislation, including the Computer Misuse Act of 1990[59] and implementation of the European Arrest Warrant to extraditions. The chapter also explores the US's approach to fraud through its enactment of the Computer

---

57 Snyder, 'Literature review as a research methodology' 338.

58 Chapter 4.

59 This creates three distinct criminal offenses: Unauthorized access to computers, including the illicit copying of software held in any computer. This carries a penalty of up to six months' imprisonment or up to a £5000 fine and will be dealt with by a magistrate. This covers hobby hacking and, potentially, penetration testing. Unauthorized access with intent to commit or facilitate commission of further offenses (such as fraud or theft), which covers more serious cases of hacking with a criminal intent. This has a penalty of up to five years' imprisonment and an unlimited fine. Because it is a serious offense, it will be a trial by jury (12 jolly good people).
Unauthorized modification of computer material, which includes the intentional and unauthorized destruction of software or data; the circulation of 'infected' materials online ('viruses'); and the unauthorized addition of a password to a data file ('crypto viruses'). This offense also carries a penalty of up to five years' imprisonment and an unlimited fine. It is also a serious offense, so it too will be a trial by jury.

Fraud and Abuse Act (CFAA), other cyber legislation and indictments linked to the prosecution of cyber offences.

Chapter 5 addresses the rule of law, the *aut dedere aut judicare* principle and Mutual Legal Assistance.[60] The examined issues include: no offence existing at the date of the extradition together with prescription and its effect. Precedential law is also discussed in tandem with the duty of extraditing or prosecuting. Other examined issues include: mutual legal assistance and the issues arising from trans-border investigations, sovereignty,[61] and practices that transcend the possible limitations anticipated in the Convention on Cybercrime.[62]

Chapter 6 basically entails a summary of the main findings and some improvement-oriented recommendations. The chapter also documents the need for integrated domestic and intercontinental synergism that validates the findings and recommendations,[63] with emphatic attention drawn to implementation enforcement.

1.8 Conclusion

The Electronic Communications and Transactions Act[64] was enacted to render the regulation of, and promotion of universal access to electronic transactions and communications tenable, and to also prevent abuse of such information.[65] Chapter XI11 of the Electronic Communications Transactions Act deals with cybercrimes, while Chapter VIII addresses Protection of Personal Information. The new Cybercrimes Act 19 of 2020 establishes specific infractions which affect cybercrime, criminalises disclosure of injurious data messages, and caters for interim protection orders; while also regulating jurisdiction and aspects accruing to mutual assistance regarding cyber and digital crimes.[66]

The digital universe parallels the universe we live in, except for its cluttered troves of past obliterated information, of data and certitudes. It is a ‘silicon

---

60 Chapter 5.
61 Strafgesetzbuch [Swiss Criminal Code] (Switzerland 21 December 1937) SR 311.0, art 271(1).
62 Trans-border Group of the Cybercrime Convention Committee (T-CY).
63 London, ‘Comparative data protection and security law’ 4.
64 Act 25 of 2002.
65 Preamble to Act 25 of 2002
66 Preamble to Act 19 of 2020.

twilight zone', with every one of us having a digital doppelgänger that is a speculum of our memoirs which will outlive us.[67] The implementation of the POPI Act[68] means that enforcement is imminent. It is important for South Africa to explore the jurisdictions of the UK and the US for direction and guidance in digital crimes, protection of personal information; as well as investigations and prosecutions which concomitantly impact on the suitability and appropriateness of extraditions.

Extradition is not a game of diplomacy, nor is it an inconsequential sideshow. Rather, it is at the very heart of winning against malefactors and defeating[69] their nefarious aspirations. The importance of extradition is the key to international law enforcement, respect for law and order,[70] and is discussed in the ensuing Chapter 2.

---

67 David H Holtzman, *Privacy Lost: How Technology is Endangering your Privacy* (Jossey-Bass 2006) xxi.

68 Act 4 of 2013.

69 International Law: The Importance of Extradition <https://www.govinfo.gov/content/pkg/CHRG-106hhrg63238/html/CHRG-106hhrg63238.htm> accessed 20 April 2020 6.

70 International Law: The Importance of Extradition 4.

Chapter 2: Extradition

2.1 Introduction

The Extradition Act[1] directs the governance of South Africa's extradition processes.[2] A Model Treaty on Extradition was endorsed by the United Nations' General Assembly in 1990 and encompassed several principles serving as a 'useful framework' for reference by States regarding extraditable offences when negotiating and revising bilateral agreements.[3] The double criminality principle commands that the alleged extraditable offence should in fact be a crime in both the requested and the requesting State.[4] It is unrequired for the infraction to be of the same name in both states, but must be substantially similar.[5] Extradition agreements were complicated during the apartheid era due to political isolation until the situation changed with South Africa's emergence from international isolation in 1994.[6] Extradition law and practices involve international law and politics, criminal law, and human rights. As such, the extradition process involves not only the judicial branch, but also the executive branch of government in most jurisdictions.[7] The process of extradition is a bilateral agreement between two sovereign States for surrendering an individual based on the request of another sovereign State for such extradition.[8] The proceedings of extraditions are regarded as sui generis in nature and do not conform to descriptions of criminal proceedings.[9] The extradition process must be followed, and illegal deportation[10] or abduction[11] should never be considered as an option for the securance of fugitives.[12]

---

1 Extradition Act 67 of 1962.
2 Watney, 'A South African perspective on mutual legal assistance' 292.
3 UN General Assembly, 'Model Treaty on Extradition: Resolution / adopted by the General Assembly' (14 December 1990) A/RES/45/116 <https://www.refworld.org/docid/3b00f18618.html> accessed 7 June 2020. Also see Dugard, Du Plessis and Katz, *International Law* 219.
4 Dugard, Du Plessis and Katz, *International Law* 214.
5 Dugard, Du Plessis and Katz, *International Law* 219.
6 Anton Katz, 'The incorporation of extradition agreements' (2003) 16 SACJ 311-322.
7 Katz, 'The incorporation of extradition agreements' 311-322.
8 Katz, 'The incorporation of extradition agreements' 311-322.
9 *Minister of Justice v Additional Magistrate, Cape Town* 2001 para 33; (*Director of Public Prosecutions: Cape of Good Hope v Trevor Claud Robinson* Case No 15/04).
10 *Mohamed and Another v President of the Republic of South Africa and Others* (CCT 17/01) [2001] ZACC 18; 2001 (3) SA 893 (CC); 2001 (7) BCLR 685 (CC) (28 May 2001) [69].

Double criminality is a substantive requirement for extradition and derives from reciprocity in respect of equivalent mutual treatment based on the mutuality of legal imperatives.[13] The below-cited excerpt attests to the affinity between the double criminality rule and reciprocity:

> The validity of the double criminality rule has never seriously been contested, resting as it does in part on the basic principle of reciprocity, which underlies the whole structure of extradition, and in part on the maxim of *nulla poena sine lege*. For the double criminality rule serves the most important function of ensuring that a person's liberty is not restricted as a consequence of offences not recognised as criminal by the requested State. The social conscience of a State is also not embarrassed by an obligation to extradite a person who would not, according to its own standards, be guilty of acts deserving punishment. So far as the reciprocity principle is concerned, the rule ensures that a State is not required to extradite categories of offenders for which it, in return, would never have occasion to make demand.[14]

2.2 Extradition

2.2.1 Extradition definition and procedures

2.2.1.1 Definition

Extradition is viewed as 'the delivery of an accused or convicted individual to the state where he is accused of, or has been convicted of a crime, by the state on whose territory he happens to be for that time'.[15] The challenge that emerges is how could the delivery of an accused be guaranteed in the event of the alleged wrongdoer being outside the borders of the State in where the crime was committed and its attendant effects were felt as well.[16] The requesting State and its law enforcement authorities are not entitled to enter the territorial

---

11 *S v Ebrahim* (279/89) [1991]; 1991 (2) SA 553 (AD); [1991] 4 All SA 356 (AD) (26 February 1991) [6].

12 Leonard, 'Extradition outgoing extraditions - Part 2' 30-31.

13 M Cherif Bassiouni, *International Extradition United States Law and Practice* (5th edn, Oxford University Press 2007) Chapter VIII B at 490.

14 Ivan Anthony Shearer, *Extradition in International Law* (Manchester University Press 1971) 137-138.

15 Dugard, Du Plessis and Katz, *International Law* 214, refers to R Jennings and A Watts (eds), *Oppenheim's International Law* (8th edn, Oxford University Press 1955) 948.

16 Watney, 'A South African perspective on mutual legal assistance' 307.

jurisdiction of another State and simply abduct the alleged perpetrator.[17] Nor are they allowed to enter such territory and just collect evidence, as this in itself would constitute a transgression in international law.[18] Such behaviour could only constitute a transgression by non-interference in another State's internal affairs.[19] That a sovereign state exercises its own territorial jurisdiction also implies that the particular country must not be seen as interfering in the domestic affairs of another country.[20] The appropriate and acceptable procedure is that the requesting State must ask the requested State for collaboration and cooperation based on mutual legal assistance for obtaining evidence relevant to the extradition of the alleged perpetrator.[21] In the *Patel* case the court pronounced thus:

> [T]he principle of double (or dual) criminality is internationally recognised as central to extradition law. The principle requires that an alleged crime for which extradition is sought is a crime in both the requested and requesting States. In other words, the crime for which extradition is sought must be one for which the requested State would in turn be able to demand extradition.[22]

Meanwhile, Oppenheim intimates:

> No person may be extradited whose deed is not a crime according to the criminal law of the State which is asked to extradite as well as the State which demands extradition.[23]

2.2.1.2 Procedures

International and domestic laws basically govern processes attendant to requests for the surrender of a wanted fugitive.[24] In such situations, there ought to be compliance with a particular State's own internal laws prior to the

---

17 *S v Ebrahim* (279/89) [1991]; 1991 (2) SA 553 (AD); [1991] 4 All SA 356 (AD) (26 February 1991). As a result, the Appellate Division set aside the conviction of treason and the sentence of 20 years imprisonment imposed by the trial court.

18 Watney, 'A South African perspective on mutual legal assistance' 293.

19 Watney, 'A South African perspective on mutual legal assistance' 293.

20 Watney, 'A South African perspective on mutual legal assistance' 293.

21 Watney, 'A South African perspective on mutual legal assistance' 293.

22 *Patel v National Director of Public Prosecutions* (NDPP) (838/2015) [2016] ZASCA 191; 2017 (1) SACR 456 (SCA) (1 December 2016) [8] (hereinafter referred to as *Patel* 2016).

23 *Patel* 2016; L Oppenheim, *International Law* (8th edn, Longmans 1955) 701.

24 Watney, 'A South African perspective on mutual legal assistance' 298.

requested State surrendering the requested fugitive individual.[25] In South Africa, the Extradition Act of 1962 is the primary regulator of extraditions.[26]

The procedures prescribed in the Act must be complied with, prior to the sought person's surrendered to the foreign or requesting State. Section 3(1) of the Act is applicable to any individual accused or convicted of an extraditable transgression committed within the territorial authority of another State which is privy to an agreement of extradition with South Africa, is liable for surrender to the State making such a request. Section 3(2) was amended and declared constitutional,[27] which applies to any who is accused or convicted for an extraditable infraction perpetrated within the jurisdictional authority of another State that is not a signatory to an agreement of extradition agreement, and shall be liable to surrender on the proviso that the President has consented to such surrender in writing.[28] An individual could be held liable to extradition in the event that another State making such a request was 'designated' by the President.[29]

The Minister of Justice obtains the request for extradition from another State through diplomatic avenues.[30] Prior to December 2020, the situation was that the Minister would notify a magistrate, who would then issue the requested arrest warrant.[31] However, section 5(1)(*a*) of the Act was viewed as inconsistent with the Constitution, thus, invalid.[32] It was argued that mere receipt of the notification stripped a judicial officer of the discretionary authority of deciding whether or not to issue a warrant.[33] All persons appearing at an extradition

---

25 *Harksen v President of the Republic of South Africa and Others* (CCT 41/99) [2000] ZACC 29; 2000 (2) SA 825 (CC); 2000 (1) SACR 300; 2000 (5) BCLR 478 (30 March 2000) [4] (hereinafter referred to as the *Harksen* case).

26 Extradition Amendment Act 67 of 1962.

27 *Harksen* case [28].

28 Extradition Amendment Act 77 of 1996 - *GG* 17589 1.

29 Section 3(*b*) of Act 77 of 1996 inserted subsec (3) of s 3 of the Act which reads as follows:
'Any person accused or convicted of an extraditable offence committed within the jurisdiction of a designated State shall be liable to be surrendered to such designated State, whether or not the offence was committed before or after the designation of such State and whether or not a court in the Republic has jurisdiction to try such person for such offence.'

30 Extradition Act 67 of 1962, s 4.

31 Extradition Act 67 of 1962, s 5.

32 *Smit v Minister of Justice and Correctional Services and Others* [2020] ZACC 29 Order 9.

33 *Smit v Minister of Justice and Correctional Services and Others* [2020] ZACC 29 [7].

inquiry can apply for bail, irrespective of the crime in term of section 60 of the Criminal Procedure Act (CPA).[34]

Section 9(1),[35] makes provision for any detained individual for the purposes of extradition to be brought before a magistrate expeditiously, who should necessarily make an inquiry for determining the appropriateness of surrendering such persons to the affected foreign jurisdiction. Section 9(2)[36] provides for the procedure to be followed and the powers which may be exercised by a magistrate at such inquiry.[37]

Pursuant to section 10,[38] a magistrate's finding of the adequacy of evidence constitutes justifiable premises to surrender the individual concerned, in the event of which the Minister of Justice could apply his/ her discretion as enjoined by section 11[39] to authorize the requested individual's surrender to any person designated by the requesting State to receive such an individual.[40] The magistrate's role is important insofar as screening purposes for determining the sufficiency or otherwise of the evidence to justify prosecution of the said individual in the requesting State.[41] The decision concerning an individual's extradition is fundamentally an executive function, which has been deeply criticised.[42] An individual's committal pursuant to a magistrate's order under section 10 is appealable to the High Court within fifteen days of such an order.[43]

2.2.2 Extradition Act 67 of 1962 and agreements

The withdrawal of South Africa from the Commonwealth in 1961 caused the country's involvement in extradition treaties to lapse in several of its extradition agreements with other Stares in the Commonwealth.[44] Before 1961, agreements of extradition between South Africa and other States within the

---

34 Criminal Procedure Act 51 of 1977, s 177.
35 Extradition Act 67 of 1962.
36 Extradition Act 67 of 1962.
37 John van der Berg, 'Notes on an aspect of extradition' 1987 Journal for Juridical Science 202.
38 Extradition Act 67 of 1962.
39 Extradition Act 67 of 1962.
40 *Harksen* case [14].
41 Extradition Act 67 of 1962, s 10(1).
42 Watney, 'A South African perspective on mutual legal assistance' 301.
43 Section 13(1) of the Act.
44 *Harksen* case [3].

Commonwealth were conducted through the British Fugitive Act of 1881.[45] Extraditions between South Africa and the Non-Commonwealth States were governed by the British Extradition Acts of 1870 to 1906, allowing the for the expansion of treaties.[46] After 1961, the British government entered into agreements under the Extradition Act of 1870 and the Seals Act of 1934 respectively.[47] The Extradition Act 67 of 1962 was then enacted, and still governs South Africa's relations on various extraditions.[48]

Presently, South Africa has treaties with many countries.[49] In 2003, the country was also a signatory to the 1957 multilateral European Convention on Extradition and became party to an agreement on extraditions with an added number of 50 States,[50] which secures returning of criminals between, and among signatory States.[51] In *Mohamed and Another v President of the Republic of South Africa and Others*,[52] the South African Constitutional Court (ConCourt) made a pronouncement regarding the nature of extraditions thus:

> It involves three elements: acts of sovereignty on the part of two States; a request by one State to another State for the delivery to it of an alleged criminal; and the delivery of the person requested for the purposes of trial and sentencing in the territory of the requesting State.

In *President of the Republic of South Africa and Others v Quagliani*,[53] the Constitutional Court acknowledged that extradition involved more than international relations or reciprocity:

---

45 Dugard, Du Plessis and Katz, *International Law* 214.

46 33 & 34 Vict c 52 (1870), 36 and 37 Vict c 60 (1873), 58 &59 Vict c 33(1895), 6 Edw VII c 15, 1906; also see Dugard, Du Plessis and Katz, *International Law* 215.

47 Act 70 of 1934, s 7.

48 Dugard, Du Plessis and Katz, *International Law* 215.

49 Department of Justice and Constitutional Development 'International Legal Obligations' <https://www.justice.gov.za/ilr/mla.html> accessed 20 July 2020.

50 Council of Europe 'European Convention on Extradition' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/024/signatures?p_auth=fYhfKTof> accessed 20 July 2020.

51 *Harksen* case [4].

52 *Mohamed and Another v President of the Republic of South Africa and Others* (CCT 17/01) [2001] ZACC 18; 2001 (3) SA 893 (CC); 2001 (7) BCLR 685 (CC) (28 May 2001) [29].

53 *President of the Republic of South Africa and Others v Quagliani; President of the Republic of South Africa and Others v Van Rooyen and Another; Goodwin v Director-General, Department of Justice and Constitutional Development and Others* (CCT24/08, CCT52/08) [2009] ZACC 1; 2009 (4) BCLR 345 (CC); 2009 (2) SA 466 (CC) (21 January 2009) [1].

> Extradition law thus straddles the divide between state sovereignty and comity between states and functions at the intersection of domestic law and international law.

States conclude extradition agreements to facilitate such extraditions between, and among themselves. However, in the absence of an agreement, requests for extraditions may be done on the basis of comity (the goodwill among states). Notwithstanding, section 3(2) of the Extradition Act invokes the President's consent to extradition when an agreement is absent.[54] In the *Harksen* case, the ruling of the court was that the consent of the President was invalid in view of section 231's provision in the Constitution,[55] and found it did not, thus rejecting the argument of the Appellant.[56]

According to section 2 of the Act, the President is empowered to make extradition agreements with other countries.[57] Amendment of the South African Extradition Act permits extradition to another country so designated by the President without the requirement of an agreement of extradition agreement.[58] South Africa's consent to the European Convention on Extradition of 1957[59] and its additional protocols is exemplary. However, such an agreement maybe

---

54 Leonard, 'Extradition outgoing extraditions - Part 2' 30-31.

55 Constitution of the Republic of South Africa, 1996.
Section 231 reads:
'(1) The negotiating and signing of all international agreements is the responsibility of the national executive.
(2) An international agreement binds the Republic only after it has been approved by resolution in both the National Assembly and the National Council of Provinces, unless it is an agreement referred to in subsection (3).
(3) An international agreement of a technical, administrative or executive nature, or an agreement which does not require either ratification or accession, entered into by the national executive, binds the Republic without approval by the National Assembly and the National Council of Provinces, but must be tabled in the Assembly and the Council within a reasonable time.
(4) Any international agreement becomes law in the Republic when it is enacted into law by national legislation; but a self-executing provision of an agreement that has been approved by Parliament is law in the Republic unless it is inconsistent with the Constitution or an Act of Parliament.
(5) The Republic is bound by international agreements which were binding on the Republic when this Constitution took effect.'

56 *Harksen* case [19].

57 Act 67 of 1962.

58 Act 67 of 1962, s 2(1)(*b*) as amended by Act 77 of 1996. '(2) Any person accused or convicted of an offence contemplated by subsection (2) of section 2 and extraditable offence committed within the jurisdiction of a foreign State which is not a party to an extradition agreement shall be liable to be surrendered to such foreign State, if the State President has in writing consented to his or her being so surrendered.'

59 *GG* 24872 of 13 May 2003.

insufficient, and South Africa should consider membership of the European Union.

2.2.3 Double criminality principle

Section 3(1) of the Act,[60] establishes that:

> Any person accused or convicted of an offence included in an extradition agreement and committed within the jurisdiction of a foreign State a party to such agreement, shall, subject to the provisions of this Act, be liable to be surrendered to such State in accordance with the terms of such agreement...

The Magistrate has to be satisfied that the conduct alleged by another State must also be regarded as criminal in South Africa as well.[61] The practice requires parties' consideration that the sentence is higher than any particular form of severity, but not name the extraditable transgression.[62] Boister argues that double criminality is not adequate by itself. The offence must also be recognised as extraditable by both States,[63] as a treaty could list these offences or eliminate those that are minor. Both approaches indicate agreement on the seriousness to warrant an extradition. A determination of the liability of an individual's surrender to a requesting State, based on an extradition agreement is incumbent on the magistrate finding that the transgression allegedly committed in a foreign State is in fact an 'extraditable offence' as determined in the Act, which makes it imperative for the infraction to be considered as such in both the requested and requesting States.[64] The most critical question, then, becomes: At which stage does the transgression become extraditable?[65]

---

60 Extradition Act 67 of 1962.

61 *Geuking v President of the Republic of South Africa* (CCT35/02*)* [2002] ZACC 29*;* 2003 (3) SA 34 (CC*)* [45] (hereinafter referred to as the *Geuking* case).

62 Extradition Act 67 of 1962, s 1 defines 'extraditable offence' means any offence which in terms of the law of the Republic and of the foreign State concerned is punishable with a sentence of imprisonment or other form of deprivation of liberty for a period of six months or more but excluding any offence under military law which is not also an offence under the ordinary criminal law of the Republic and of such foreign State.

63 Neil Boister, 'The trend to "universal extradition" over subsidiary universal jurisdiction in the suppression of transnational crime' (2003) 1 Acta Juridica 287-313.

64 *Patel v S* (A101/2014) [2015] ZAGPJHC 188; [2015] 4 All SA 382 (GJ); 2016 (2) SACR 141 (GJ) (18 August 2015) [21] (hereinafter referred to as *Patel* 2015).

65 *Patel* 2015 [21].

2.3 Double criminality principle through case law and extraditable offences

2.3.1 Development of our law in respect of the double criminality principle and case law

Section 3 of the Extradition Act[66] has caused some controversy as to whether the extradition request should constitute a crime in South Africa when the request for extradition is made, or at the time of the alleged infraction itself. This appears to have a two-fold implication:

i) Firstly, whether the extradition request must be considered a crime in South Africa at the time of the extradition request; or

ii) Secondly, or at the time of the alleged offence.

This section of the Act does not specifically, address the issue of whether the extradition request is a crime in South Africa at the time of the request for extradition, or at the time of the alleged transgression. This raises a problem where extradition is sought in respect of a specific cybercrime offence not covered by the common law or the ECT Act.[67] On 26 May 2021, the President signed the Cybercrimes Bill into law, with 'certain sections' being implemented on the '1 December 2021',[68] but the rest of the Cybercrimes Act will only come

---

66 'Persons liable to be extradited -
(1) Any person accused or convicted of an offence included in an extradition agreement and committed within the jurisdiction of a foreign State a party to such agreement, shall, subject to the provisions of this Act, be liable to be surrendered to such State in accordance with the terms of such agreement, whether or not the offence was committed before or after the commencement of this Act or before or after the date upon which the agreement comes into operation and whether or not a court in the Republic has jurisdiction to try such person for such offence.
(2) Any person accused or convicted of an extraditable offence committed within the jurisdiction of a foreign State which is not a party to an extradition agreement shall be liable to be surrendered to such foreign State, if the President has in writing consented to his or her being so surrendered.
(3) Any person accused or convicted of an extraditable offence committed within the jurisdiction of a designated State shall be liable to be surrendered to such designated State, whether or not the offence was committed before or after the designation of such State and whether or not a court in the Republic has jurisdiction to try such person for such offence.'

67 Electronic Communications and Transactions Act 25 of 2002 446; *GG* 23809 of 30 August 2002.

68 'President's Minute No. 334/2021, dated 19/11/2021.
Chapter 1 (Definitions and Interpretations).
Chapter 2 (Cybercrimes) (Parts I to V only).

into force on a date determined by the President through proclamation in the Gazette.[69] There is no certainty about the much-needed promulgation of cybersecurity legislation. The definition of the extraditable offence[70] encompasses infractions that were committed prior to, or subsequent to the Extradition Act, or before or after the date upon which, it would appear a bilateral agreement comes into force. The challenge emerges in the event when legislation has not been enacted, and there is no commission of an extraditable infraction. Section 7(1)[71] and section 35(3)[72] of the Constitution elevates the right to a fair trial for all citizens in the country. Accordingly, the same maxim should also prevail in extraditions and the requirement for double criminality.

2.3.1.1 Ex parte Pinochet Ugarte (No 3)

The facts of the above-cited case were summarized by the court; the Applicant was Chile's former head of state who was arrested while visiting in London through the agency of a metropolitan stipendiary magistrate's provisional warrant issued according to section 8 of the Extradition Act of 1989 after the issuance of an international arrest warrant by the Central Court of Criminal Proceedings, No 5, in Madrid. Six days thereafter, a magistrate issued another warrant in respect of section 8 of the self-same Extradition Act after receiving

---

Chapter 3 (Jurisdiction).
Chapter 4 (Powers to Investigate, Search, Access or Seize (except sections 38(1)(*d*)-(*f*), 40(3)-(4), and (41-44).
Chapter 7 (Evidence)
Chapter 8 | Reporting Obligations and Capacity Building (except section 54).
Chapter 9 (General Provisions) with the exclusions of sections 11B-D, and 56A(3)(*c*)-(*e*) of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, in the Schedule of laws repealed or amended in terms of section 58.'

69 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read' (2021) <https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa> accessed 2 June 2021.

70 Act 67 of 1962, s 3.

71 'Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom'.

72 'Every accused person has a right to a fair trial, which includes the right:
- to be informed of the charge with sufficient detail to answer it;
- to have adequate time and facilities to prepare a defence;
- to a public trial before an ordinary court;
- to have their trial begin and conclude without unreasonable delay.'

another international arrest warrant that a court in Spain had issued, alleging amongst other, that the Applicant had commanded his subordinate officials, during his tenure from 1973 to 1990, to commit torture; which is prescribed in section 134(1) of Chile's Criminal Justice Act of 1988 and hostage taking; which is prescribed in section 1 of that country's Taking of Hostages Act of 1982. The Applicant subsequently instituted proceedings in the Divisional Court pursuant to certiorari orders to dismiss the first provisional arrest warrant as disclosing no extraditable transgression as articulated in section 2 of Chile's Extradition Act; and that both warrants alleging the Applicant's torture and hostage-taking offences in exercising his official Head of State responsibilities and in terms of which he was rightfully entitled to be declared immune under provisions of international customary law and section 20(1) of Part III of their State Immunity Act of 1978, read jointly with articles 29, 31 and 39 of Schedule 1 of the Diplomatic Privileges Act of 1964.

The Divisional Court quashed both warrants. The appeal was heard again, and the majority ruling held that the allegation of the conduct which was pivotal to the requested extradition, must also constitute a crime under UK law and the requesting State.[73] The demand for the conduct to be considered a crime in the UK at the time of its alleged commission, and that trans-national torture did not constitute a crime in the UK until section 134 of the Criminal Justice Act, only came into force on 29 September 1988.[74] Accordingly, the court held that:

> All the alleged offences of torture and conspiracy to torture before that date and all the alleged offences of murder and conspiracy to murder which did not occur in Spain were crimes for which the Applicant could not be extradited.[75]

The dissenting view, however, was that a former Head of State was immune from the territorial criminal authority of the UK for deeds so committed in that official designation.[76] Torture is internationally regarded as a despicable crime

---

73 *Ex parte Pinochet Ugarte (No 3)* [148] para D (hereinafter referred to the *Pinochet* (No 3) case)
74 *Pinochet* (No 3) [148] para D-E.
75 *Pinochet* (No 3) [148] para D-E.
76 *Pinochet* (No 3) [148] para F. Lord Goff dissenting.

against humanity and jus cogens.[77] In 1994, the International Convention against Torture and other Cruel, Inhumane or Degrading Treatment or Punishment granted universal jurisdiction for extradition and/ or punishment of a public official involved in torture.[78] The United Kingdom, Spain and Chile had approved the Convention by 8 December 1988, and the Applicant could not be exonerated from torture or conspiracy to torture crimes following that date.[79]

The dissenting findings do not support the view of the alleged conduct to be considered a crime in the UK at the time of its alleged commission in the requesting State. Our courts further explored this issue in *Palazzolo v Minister of Justice and Constitutional Development*.[80]

2.3.1.2 Palazzolo v Minister of Justice and Constitutional Development (first Palazzolo case)

In the first Palazzolo case, the court referred to his troubled relationship with the South African authorities for more than twenty years, during which there were six requests to the South African authorities by their Italian counterparts for the extradition of the Applicant.[81] He was granted South African citizenship by automatic naturalisation on 24 January 1995.[82] The applicant was found guilty under section 416 of the Italian Criminal Code regarding the offence of complicity in aggravated Mafia-type of association and then sentenced to an imprisonment term of nine years.[83] The Appeal Court of Palermo and the Supreme Court of Appeal in Rome subsequently confirmed this conviction and subsequent sentencing of the Applicant.[84] However, the Cape High Court in South Africa upheld that there was no expression in the request that a conviction of a Mafia-type association under section 416 bis of the Italian Criminal Code held a corresponding effect in nature in the South African

---

77 Definition - the principles which form the norms of international law that cannot be set aside.
78 *Pinochet* (No 3).
79 *Pinochet* (No 3) para G-H.
80 *Palazzolo v Minister of Justice and Constitutional Development* (4731/2010) [2010] ZAWCHC 422 (14 June 2010) 4 [6] (hereinafter referred to as First *Palazzolo* case).
81 First *Palazzolo* case [1].
82 First *Palazzolo* case [2].
83 First *Palazzolo* case [3].
84 First *Palazzolo* case.

criminal law system, which then resulted in it being an un-extraditable offence.[85] Reliance on the Prevention of Organised Crime Act 121 of 1998 and the Prevention and Combating of Corrupt Activities Act 12 of 2004 was seen as misguided in the absence of these Acts being promulgated as law.[86] The court confirmed the Pinochet Ugarte case, that 'the principle of double criminality requires that the conduct for which extradition is sought, is an offence in both the requesting and requested countries at the time of the commission of the offence'.[87]

2.3.1.3 Patel Usman Ismail

The facts of the afore-cited case[88] were as follows: The USA made a request for Mr Patel's extradition. He was a US citizen resident in the Republic of South Africa (RSA) at the time of the request to be prosecuted for alleged offences committed in the US. The Appellant was then apprehended and subsequently appeared in the Randburg magistrate's court in respect of the Extradition Act.[89] It was the court's finding that the Appellant was obliged to be surrendered to the territorial jurisdiction of the USA on 15 February 2013, with a committal order issued as provided by section 10(1)[90] of the Act. The Appellant was committed to prison while awaiting the decision of the Minister of Justice concerning his surrender to the USA.[91] The core issues on the Appeal were: Firstly, whether the offences constituting the Appellant offences were in fact 'extraditable offences'. Secondly, whether the Prosecuting Authority of the USA furnished certificates that were compliant with similar pre-requisites of the South African Extradition Act, particularly section10(2).[92] The requested extradition was made

---

85 First *Palazzolo* case 17 [34].
86 First *Palazzolo* case.
87 First *Palazzolo* case.
88 *Patel* 2015.
89 Act 67 of 1962.
90 'If upon consideration of the evidence adduced at the enquiry referred to in section 9(4)(*a*) and (*b*)(i) the magistrate finds that the person brought before him or her is liable to be surrendered to the foreign State concerned and, in the case where such person is accused of an offence, that there is sufficient evidence to warrant a prosecution for the offence in the foreign State concerned, the magistrate shall issue an order committing such person to prison to await the Minister's decision with regard to his or her surrender, at the same time informing such person that he or she may within 15 days' appeal against such order to the Supreme Court.'
91 *Patel* 2015 [1]-[2]; Extradition Act 67 of 1962, s 10(1).
92 *Patel* 2015 8 [15].

in terms of an extradition treaty between the USA and the RSA.[93] The Appellant had allegedly committed banking-related crimes in the USA between 2005 to October 2007, which offences were punishable by a sentence of more than a year's imprisonment.[94] The corresponding RSA charges would be contravention of sections 28 and 29 of the Financial Intelligence Centre Act 38 of 2001, which only came into operation in 2010.[95] The magistrate relied on section 3(1) of the Act,[96] and interpreted it as covering transgressions committed before operationalisation of the Act, or transgressions committed before the treaty was concluded.[97]

2.3.2 The time issue and Bell v State

The treaty, ratified on 9 November 2000 and published in the Government Gazette,[98] does not expressly address the time issue.[99] The court in the *Patel* case stated that the principle (time issue) was profound, partially rests on both the reciprocity principle and also partially expressed in the maxim, *null poena sine lege*.[100] It was argued that the principle was fulfilled the moment the alleged offence was viewed as such in the requested State. At the same time, it was also upheld that the alleged transgressions were not viewed as such in the RSA at the time that they were allegedly committed in the USA.[101]

The Court made reference to the *Bell v State* extradition case[102] by Australia. The charges related to occurrences of more than 20 years previously, and allegedly included indecency an indecency assaults, all of which were allegedly committed in February 1977 with young boys of between 11 and 18 years of

---

93 *GG* 7100 of 29 June 2001.
94 *Patel* 2015 12 [28].
95 *Patel* 2015 6 [11.3].
96 Act 67 of 1962.
97 *Patel* 2015 7 [13]; Act 67 of 1962, s 3(1) reads 'Any person accused or convicted of an offence included in an extradition agreement and committed within the jurisdiction of a foreign State a party to such agreement, shall, subject to the provisions of this Act, be liable to be surrendered to such State in accordance with the terms of such agreement, whether or not the offence was committed before or after the commencement of this Act or before or after the date upon which the agreement comes into operation and whether or not a court in the Republic has jurisdiction to try such person for such offence.'
98 *GG* 7100 of 29 June 2001.
99 *Patel* 2015 8 [16].
100 *Patel* 2015 10 [22].
101 *Patel* 2015 10 [23].
102 *Bell v S* [1997] 2 All SA 692 (EC).

age.[103] It was the view of the Eastern Cape Division that according to South African laws, offences committed more than 20 years previously were not liable for punishment, and the offences for which the Australian authorities made requests for the extradition of Mr Bell were not offences pursuant to extradition. It was the court's view that an individual who could not be prosecuted for any offence according to South African law and could then not be charged for that offence at that stage. When Australia made the request for the extradition of Bell, there was no treaty governing extradition between itself and South Africa.[104]

2.3.3 Extraditable offences

Article 2 of the Convention[105] refers to 'extraditable offence', which can be punished in terms of the laws of the requesting State or Party, and of the requested Party by depriving liberty or a detention order for at least one year or

---

103 *Patel* 2015 12 [27] (italics – own emphasis).

104 *Patel* 2015 (italics – own emphasis).

105 European Convention on Extradition - Paris, 13.Xii.1957 art 2:

'1. Extradition shall be granted in respect of offences punishable under the laws of the requesting Party and of the requested Party by deprivation of liberty or under a detention order for a maximum period of at least one year or by a more severe penalty. Where a conviction and prison sentence have occurred or a detention order has been made in the territory of the requesting Party, the punishment awarded must have been for a period of at least four months.

2. If the request for extradition includes several separate offences each of which is punishable under the laws of the requesting Party and the requested Party by deprivation of liberty or under a detention order, but of which some do not fulfil the condition with regard to the amount of punishment which may be awarded, the requested Party shall also have the right to grant extradition for the latter offences.

3. Any Contracting Party whose law does not allow extradition for certain of the offences referred to in paragraph 1 of this article may, in so far as it is concerned, exclude such offences from the application of this Convention.

4. Any Contracting Party which wishes to avail itself of the right provided for in paragraph 3 of this article shall, at the time of deposit of its instrument of ratification or accession, transmit to the Secretary General of the Council of Europe either a list of the offences for which extradition is allowed or a list of those for which it is excluded and shall at the same time indicate the legal provisions which allow or exclude extradition.

5. If extradition is subsequently excluded in respect of other offences by the law of a Contracting Party, that Party shall notify the Secretary General. The Secretary General shall inform the other signatories. Such notification shall not take effect until three months from the date of its receipt by the Secretary General.

6. Any Party which avails itself of the right provided for in paragraphs 4 or 5 of this article may at any time apply this Convention to offences which have been excluded from it. It shall inform the Secretary General of the Council of such changes, and the Secretary General shall inform the other signatories.

7. Any Party may apply reciprocity in respect of any offences excluded from the application of the Convention under this article.'

more severe penalty in the case of a conviction and subsequent prison sentence or detention order made by the Party making such a request, and measures must have been prevalent for at least a period of four months.[106] The requested party should also be entitled to grant extradition in respect of the offences where the amount of punishment is not stated.[107] There is also provision for the exclusion of offences.[108] In the event that extradition is excluded on grounds of the law of a Contracting Party, such Party should notify the Secretary-General who then shall inform the other signatories.[109] Furthermore, any Party is entitled to apply reciprocity concerning infractions that have been excluded from applications of the Convention.[110]

The magistrate's determination of whether or not the offence is included in the agreement or treaty, should take cognizance of the treaty itself.[111] If there is no treaty in place, the magistrate should be optimally satisfied that the individual is in fact accused of an offence that is 'extraditable' within the territorial jurisdiction of the particular requesting State. The definition of 'extraditable offence' in section 1 of the Act[112] is crucial, and adequate details of the transgression should be provided to the magistrate for the determination in question to be made.[113] The court duly emphasized the construing of the treaty in conjunction with the applicable laws as required by the South African Constitution for a particular State's compliance with such laws.[114]

2.3.4 Criticisms of case law

The decision in *S v Bell* was criticized because of the absence of a treaty between South Africa and Australia, and the court did not explicitly interpret and seek to allocate meaning to the double criminality principle but found that the lapse of time in South Africa prevented the offence and its concomitant

---

106 European Convention on Extradition - Paris, 13.Xii.1957 art 2(1).
107 European Convention on Extradition - Paris, 13.Xii.1957 art 2(2).
108 European Convention on Extradition - Paris, 13.Xii.1957 art 2(3).
109 European Convention on Extradition - Paris, 13.Xii.1957 arts 2(4) and 2(5).
110 European Convention on Extradition - Paris, 13.Xii.1957 art 2(7).
111 *Patel* 2015 16 [37].
112 Extradition Act 67 of 1962.
113 *Patel* 2015.
114 *Patel* 2015 19 [41].

prosecution from constituting extraditable offences.[115] Article 10[116] refers to the time lapse thus:

> Extradition shall not be granted when the person claimed has, according to the law of either the requesting or the requested Party, become immune by reason of lapse of time from prosecution or punishment.

Accordingly, the court criticized the Bell thus:

> The court possibly went too far. It seemingly, and unwittingly, gave the definition of 'extraditable offence' in the Act and, in particular, the word 'punishable' in that definition, a meaning that is not consistent with the purpose of the Act, and more particularly, the purpose of the magistrate's enquiry in terms of the Act. The purpose is not to establish the requested person's culpability, or whether he or she has any defence to the criminal charges in the foreign State.[117]

In *Pinochet (No. 3),* the interpretation by the House of Lords in defining extradition crime in the English extradition Act was criticised[118] as rather restrictive, strained or even utterly wrong; and that the interpretation by other courts (most notably that of Lord Bingham, CJ and Lord Lloyd) was most n laudable. The House of Lords duly concluded that *the date of the extradition request was the correct time, and not the date on which the committed offence allegedly occurred in the foreign State*.[119] On appeal to the Supreme Court of Appeal, in the *Patel* case, the court concluded that the rule of double criminality should be optimally fulfilled as constituting the date for the extradition request of a fugitive, and not the date on which the alleged offense was committed in the foreign jurisdiction.[120]

---

115 *Patel* 2015 on 24 [54]; *Bell v S* [1997] 2 All SA 692 (EC) 699F-G.

116 European Convention on Extradition - Paris, 13.Xii.1957.

117 *Geuking* case.

118 Dugard, Du Plessis and Katz, *International Law* 220; J Dugard, 'Dealing with crimes of a past regime: Is amnesty still an option?' (1999) 12 Leiden Journal of International Law 1001, 1008-1009; M du Plessis, 'The Pinochet cases and South African extradition law' (2000) 16 SAJHR 669, 680; A O'Shea, 'Pinochet and Beyond: The International Implications of Amnesty' (2000) 16 SAJHR 642, 653-656; C Warbrick and D McGoldrick, 'Extradition Law Aspects of Pinochet 3' (1999) 48 International and Comparative Law Quarterly 958; E du Toit and others, *Commentary on the Criminal Procedure Act* (Juta 1993).

119 *Patel* 2015 20 [44] (italics – own emphasis).

120 *Patel* 2016.

In the second *Palazzolo* case, the application sought to vary the judgment in the first case, and judgment was subsequently delivered on 14 April 2011.[121] It was argued that the judgment concerning the double criminality principle was obiter and wrong. A probable further Italian extradition request (after six previous requests), subsequently resulted in the Applicant's apprehension and flouting of his fundamental rights.[122] The application was dismissed and Mr VR Palazzolo was subsequently not extradited from South Africa (to Italy). Notwithstanding, he was arrested in Bangkok in 2012 by Interpol and extradited to Sicily to serve his nine-year jail term.[123]

This argument of the infringement of Mr VR Palazzolo's fundamental rights was not addressed in the judgment. This raises the issue of whether unlimited requests for extradition can be made, or whether such requests can then be held in abeyance until South Africa passes laws to comply with the European Convention's Article 2[124] *in respect of an extraditable offence*.[125]

In the *Patel* case, the court intimated that interpretation of Article 2.1 of the treaty referring to the requested date, also gives effect to the intergovernmental cooperation and a treaty concerning the duties and rights of States.[126] It is a fundamental rule of the Vienna Convention on the Law of Treaties[127] that a treaty should be interpreted according to the good faith and ordinary meaning allocated to the contextual terms, purpose and object of the very treaty. The court declared that the approach to the date of the offence for double criminality would undermine cooperation between the States, negating the very purpose of a bilateral treaty of extradition to bring those who have committed serious crimes to justice.[128]

---

121 Second *Palazzolo* case.

122 Second Palazzolo case 6 [7].

123 Jade Otto, 'Court blow for alleged mafia boss' (21 December 2012) <https://www.iol.co.za/news/court-blow-for-alleged-mafia-boss-1444016> accessed 6 May 2020.

124 European Convention on Extradition - Paris, 13.Xii.1957.

125 Italics – own emphasis.

126 *Patel* 2016 16 [35].

127 Vienna Convention on the Law of Treaties (23 May 1969) <https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf> accessed 10 January 2021 article 31(1)-(2); WTO Agreement on Trade-Related Aspects of Intellectual Property Rights.

128 *Patel* 2016 17 [38].

2.3.5 Section 10(2) certificate compliance for the requirement of double criminality

A section 10(2)[129] certificate requires a magistrate's declared satisfaction with the adequacy of evidence justifying prosecution in a foreign jurisdiction. The issue then arises on whether or not the certificate of the requesting State to South Africa is vague or unclear, and whether or not this will be cogent for the Director of Prosecution to accept such a certificate and issue an Article 10(2) certificate in our Extradition Act.

The argument in the *Patel* case was rejected on grounds that the certificate ought to use the appropriate section 10(2) phraseology for it to be declared valid.[130] A foreign State is not obliged in terms of the Act to issue a certificate as contemplated, which is merely a mechanism to facilitate proof.[131] The Constitutional Court[132] held that a section 10(2) certificate is consistent with the Constitution. The court further determined that once the double criminality rule has been satisfied, the magistrate was obliged to depend on the certificate as regards the narrow question of the prosecution of the fugitive's conduct in the foreign jurisdiction, as that question would not usually be known in respect of South African lawyers' or judicial officers' expertise. An extradition enquiry is not a trial, as the process does not involve any innocence or guilt adjudication.

2.4 Summary

- Firstly, our case law[133] confirms that the double criminality principle regarding criminal transgressions applies from the date of the extradition.
- request,[134] which is a departure from the UK norm.[135] It seems that section 18 of the Criminal Procedure Act[136] applies to domestic law and refers to the time during which the offence was committed, but not for extraditions.

---

129 Extradition Act 67 of 1962. 'The magistrate shall accept as conclusive proof a certificate which appears to him or her to be issued by an appropriate authority in charge of the prosecution in the foreign State concerned, stating that it has sufficient evidence at its disposal to warrant the prosecution of the person concerned.'

130 *Patel* 2015 27 [65].

131 *Patel* 2015 29 [72].

132 *Geuking* case [45].

133 Second *Palazzolo* case.

134 *Patel* 2016.

- Secondly, is the issue of whether or not treaties are self-executing is critical, considering that section 231(4) of the Constitution looms large, and has attracted considerable jurisprudential attention.[137]

- Thirdly, there is the issue of whether or not the rule of law applies when there is no concomitant law and violation; and therefore, no 'extraditable offence'.[138] This further raises the issue of prescription, including a failed earlier attempt at extradition.[139]

- The quandary that arises is whether it can be inferred in respect of some offences of cybercrime, that there is no time limit as to *timing* of the requesting State to bring an extradition request, in terms of which some of the requests will remain pending until the Cybercrime Act is fully operational for the remainder of the sections, or until cybersecurity legislation is enacted.

  A similar argument was raised by Mr Palazzolo's counsel in the Palazollo[140] case, which endured for more than two decades between Mr Palazollo and the South African authorities.[141] The Italian government submitted six requests to their South African counterparts for the extradition of Mr Palazollo. There was no South African legislation that criminalised the complicity of an aggravated Mafia-type association, which is a crime according to section 146 bis in the Italian Criminal Code; and it was therefore, not an extraditable offence.[142]

---

135 *Pinochet* (No 3).
136 Act 51 of 1977.
137 Untalimile Crystal Amenda Mokoena and Emma Charlene Lubaale 'Extradition in the absence of state agreements: Provisions in international treaties on extradition' (2019) 67 SA Crim Q 31-42.
138 *Geuking* case.
139 *McCarthy v Additional Magistrate, Johannesburg* [2000] (2) SACR 542 (SCA); *Saliu v S* (2014/A262) [2015] ZAGPJHC 175 (25 August 2015); *Bell v State* A101/2014 ZAGPHC, Johannesburg [8]–[11].
140 Second *Palazzolo*.
141 Second *Palazzolo*.
142 Second *Palazzolo*.

Mr Palazollo's counsel argued that a further extradition request from the Italian government would trigger an arrest and violation of the applicant's basic rights.[143] This argument was not addressed in the Palazollo judgement, which raises the issue of whether or not unlimited requests for extraditions can be made, or whether these requests can be held in abeyance until a country passes laws compliant with the European Convention's Article 2.[144] The case of *S v Speedie*[145] appears to settle this issue.

- Fourthly, there is the issue of whether or not there should be an amendment to the Extradition Act[146] and its resultant effect to the double criminality rule not constituting a requirement for cybercrimes, because of the complexity of cybercrimes, their volatile nature and lack of global uniformity.

2.5 Conclusion

The twentieth century has provided for the freedom of movement of persons, commodities, services, improvement in transport and telecommunications, but also inadvertently created a conducive opportunity for the globalization of culture, commerce and crime,[147] and which has also created a jurisdiction challenge. Once criminal jurisdiction of a State is established, the extradition process allows it to lawfully acquire custody over an individual criminal who has fled to, or who is located in another jurisdiction.[148] States were always concerned with pursuing such individuals who have committed domestic crimes and then flee to other jurisdictions in which they have not committed crime to warrant prosecution. Porous transnational borders have contributed to easy flight from justice by wanted offenders.[149] Before an extradition can be considered, an extraditable crime must have been committed.[150] As determined in section 1 of the South African Extradition Act, it includes any conduct which

---

143 Second *Palazzolo*.
144 European Convention on Extradition - Paris, 13.Xii.1957.
145 (444/83) [1985] ZASCA 1; [1985] 2 All SA 112 (A) (12 March 1985).
146 Act 67 of 1962.
147 Boister, 'The trend to "universal extradition"' 287.
148 Boister, 'The trend to "universal extradition"' 296.
149 Boister, 'The trend to "universal extradition"' 288.
150 Leonard, 'What is extradition? Part 1' 30-31.

constitutes a crime according to both South African law and that of the foreign State concerned;[151] the so-called dual criminality principle. The European Convention on Extradition's Article 12[152] prescribes procedures that ought to be followed, in terms of which the request ought to be written and communicated diplomatically, with original documents, or authenticated copies thereof, a statement of the offenses accompanied by the relevant or applicable law.[153]

The principle of double criminality is therefore, closely related to extraditable offences.[154] This must be evident from the provisions of both the Act and the Treaty. Article 2(1) of the Convention[155] states that the relevant offence should be penalised in respect of the laws of the requesting and the requested parties,[156] which is the due requirement for double criminality. In cases where South Africa is duty-bound by its commitment to a treaty of extradition, the terms of such a treaty should regulate the applicable international obligations.[157] Meanwhile, internal law is concerned with implementation of such international obligations in accordance with the provisions of the Act, including a non-treaty extradition.[158]

The return of criminals is secured by using extradition agreements between States,[159] bearing in mind that the Extradition Act 67 of 1962 still governs the

---

151 Extradition Act 67 of 1962.

152 *GG* 24872 of 13 May 2003.

153 '(1) The request shall be in writing and shall be communicated through the diplomatic channel. Other means of communication may be arranged by direct agreement between two or more Parties.
(2) The request shall be supported by:
(*a*) The original or an authenticated copy of the conviction and sentence or detention order immediately enforceable or of the warrant of arrest or other order having the same effect and issued in accordance with the procedure laid down in the law of the requesting Party;
(*b*) A statement of the offences for which extradition is requested. The time and place of their commission, their legal descriptions and a reference to the relevant legal provisions shall be set out as accurately as possible; and
(*c*) A copy of the relevant enactments or, where this is not possible, a statement of the relevant law and as accurate a description as possible of the person claimed, together with any other information which will help to establish his identity and nationality.'

154 Bassiouni, *International Extradition* 491.

155 European Convention on Extradition - Paris, 13. Xii. 1957.

156 First *Palazzolo* case 4 [6].

157 Boister, 'The trend to "universal extradition"' 305.

158 *Harksen* case [14].

159 *Harksen* case [4].

country's extradition relations.[160] The amendment of the South African Extradition Act allows for extradition to a country that has been designated by the President in the absence of an extradition agreement.[161] However, there have been serious concerns raised to guide the extradition exemptions because of status or preference[162] and a disregard for the rule of law, despite prevalence of the treaties.

The double criminality doctrine underlies extradition processes.[163] Article 2 of the Convention[164] refers to an extraditable offence that is punishable in both the laws of the requested State and the requesting State, with an order of detention for a period that does not exceed one year, or more severe penal measures. 'A request for extradition is not a request for transfer of jurisdiction, nor a request for a trial but a request to assist the appropriate jurisdiction in rendering its justice.'[165] Its purpose is to ensure that the freedom of persons is un-curtailed because of offences not recognised as such by the requested State.[166] The

---

160 Dugard, Du Plessis and Katz, *International Law* 215.

161 Section 2(1)(*b*) of Act 67 of 1962, as amended by Act 77 of 1996.
'(2) Any person accused or convicted of an offence contemplated by subsection (2) of section two and extraditable offence committed within the jurisdiction of a foreign State which is not a party to an extradition agreement shall be liable to be surrendered to such foreign State, if the State President has in writing consented to his or her being so surrendered.'

162 The anomaly arises is failure to respect the rule of law, where the United Nations Committee noted the 'failure to detain Omar al-Bashir, President of the Sudan, in June 2015 pursuant to an International Criminal Court arrest warrant, to be inconsistent with the Constitution and expresses concern that President Al-Bashir was authorized to leave the country in violation of an interim court order'.
K Ramjathan-Keogh, 'South Africa, Apartheid, Crimes against humanity and the Rule of Law: Quo Vadis' Daily Maverick (21 February 2020) <https://www.dailymaverick.co.za/article/2020-02-21-south-africa-apartheid-crimes-against-humanity-and-the-rule-of-law-quo-vadis/> accessed 5 April 2020.
The case of the former head of Rwandan intelligence, Kayumba Nyamwasa, from June 2010 is another case of the disregard of the rule of law. South Africa granted him refugee status where he was implicated in the commission of egregious crimes and is the subject of various extradition requests.
United Nations (UN) Report March 2016 'International Covenant on Civil and Political Rights' <http://docstore.ohchr.org/SelfServices/FilesHandler.Ashx?Enc=6QkG1d%2fPPRiCAqhKb7yhsowwsSwFehBWX2ZjedBh4%2f811AqGyI2MTdng6xdE8vcB81uWeU1SfkzAjkFApm4n4sVMY4cvhDsmlet3UuCiWMpSKAPdJOaa%2bhTfv%2fQXEkwx> accessed 20 October 2020.

163 First *Palazzolo* case 10 [4].

164 European Convention on Extradition - Paris, 13.Xii.1957.

165 *Patel* 2015 [54], [56]. The argument of the European countries who are parties to the European Convention on Extradition, who adopt an '*in abstracto*' interpretation of art 2 of the Convention.

166 Dugard, Du Plessis and Katz, *International Law*, refers to Shearer, *Extradition in International Law* 137.

issue of double criminality was settled by the Supreme Court of Appeal (SCA) in *Patel*, where the court concluded that the rule pertinent to double criminality ought to be satisfied at the date of the extradition request for a fugitive, and not of the date the alleged crime is supposed to have been committed in the foreign jurisdiction.[167] In December 2020,[168] the Constitutional Court has declared section 5(1)(*a*) unconstitutional. That brings an end to a magistrate issuing a warrant of arrest upon receiving notification from the Minister concerning a request for the surrender of a person from a foreign jurisdiction.[169]

The double criminality principle is, of course, only of any use if the offence it references is in both countries and is sufficient to warrant extradition. The next chapter explores the selected cyber legislation in South Africa and determines whether or not it is adequate to comply with the double criminality principle as required by the respective extradition prescripts.

---

167 *Patel* 2016.

168 *Smit v Minister of Justice and Correctional Services and Others* 2021 (3) BCLR 219 CC; 2021(1) SACR 482 CC.

169 *Smit v Minister of Justice and Correctional Services and Others* [2020] ZACC 29 para 7.

Chapter 3: South Africa's cyber laws

3.1 Introduction

Cybercrime is not specifically defined in section 1 of the Cybercrime Act 19 of 2020, but instead incorporates the definition of 'article' to include 'data, computer program, a data storage medium and a computer system'. The definition of 'computer' has also been given a wide definition to include 'any electronic programmable device'. Cybercrime very simplistically put, refers to computer crime, using a computer to commit criminal offences, and is extensively defined to keep up with technology.

Innovation in technology, and quick gain to boundless on-line digital data, imply the gradual lack of importance of jurisdictions for countries.[1] The chapter focuses on some of our cybercrime legislation, and whether such legislation is compliant with international expectations and standards. This chapter interrogates some of the prevalent laws regarding South African cybercrime, namely: the common law, the Electronic Communications and Transactions Act (ECT Act),[2] the South African Police Service Act (SAPS Act),[3] Correctional Services Act,[4] the National Prosecuting Authority Act,[5] the Financial Intelligence Centre Act,[6] the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA),[7] and South Africa's Protection of Personal Information Act (POPI Act).[8] The Cybercrime Act,[9] once in operation, will repeal sections 85, 86, 87, and 88 of the ECT Act.

There have also been criticisms regarding the Cybercrime Bill and its extent of addressing Extradition of cybercrime offences. The President signed the

---

1 BusinessTech 'Stay vs leaving the country – what young South African workers plan to do' (12 March 2021) <https://businesstech.co.za/news/business/475468/stay-vs-leaving-the-country-what-young-south-african-workers-plan-todo/?utm_source=everlytic&utm_mediu m=newsletter&utm_campaign=businesstech> accessed 12 March 2021.

2 Act 25 of 2002.

3 Act 68 of 1995.

4 Act 111 of 1998.

5 Act 32 of 1998.

6 Act 38 of 2001.

7 Act 70 of 2002.

8 Act 4 of 2013.

9 Act 19 of 2020

Cybercrimes Bill into law,[10] but the remainder of the sections in the Cybercrimes Act can only be operationalised by a gazetted proclamation.[11] The Act does not refer to cybersecurity, compared to its first publication in 2015 as the Cybercrimes and Cybersecurity Bill.

3.2 Types of cybercrime laws

3.2.1 Common law offences of fraud and theft

Fraud[12] and theft[13] are common law offences that are still relied on, in the context of cybercrimes, the most common of which are identity theft, hacking and denial-of-service infringements.[14] The prosecution of identity theft is either fraud-based on misrepresentation, or according to section 18[15] of the Identification Act.[16] Identity theft in South Africa is generally prosecuted within the realm of the common law;[17] in terms of which an individual convicted of identity theft could be charged with forgery, fraud and utterance of a forged document, pending the case's circumstances. It is submitted that in South Africa, existing legislation is inadequate to deal with the scourge of identity theft,[18] which is anticipated to increase into the unforeseeable future, mostly due to a plethora of existing databases containing vital personal information. Many of these databases do not even have adequate security, especially for consumer protection.[19]

---

10 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read' (2021) <https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa> accessed 2 June 2021.

11 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read'.

12 Carel R Snyman, *Criminal Law* (5th edn, LexisNexis 2008) 520 defines fraud as 'the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another'.

13 John Milton and MA Hunt, *South African Criminal Law and Procedure* (3rd edn, Juta 1996) 566 defines theft as '…an unlawful *contrectatio* with intent to steal of a thing capable of being stolen'.

14 Marco Gercke, 'Understanding cybercrime: phenomena, challenges and legal response' (November 2014) <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf> accessed 30 December 2020.

15 Section 18(1)(*d*): 'No person shall— (*d*) having come into possession of an identity card, a certificate or a temporary identity certificate belonging to another person, present it as his or her own or belonging to any person other than the person to whom it belongs'.

16 Act 68 of 1997.

17 Basdeo, 'Criminal and Procedural Legal Challenges' 363.

18 Basdeo, 'Criminal and Procedural Legal Challenges' 368.

19 Basdeo, 'Criminal and Procedural Legal Challenges' 366.

3.2.2 Electronic Communications and Transactions Act (ECTA)[20]

The ECT Act impacts on electronic communications and relates to any form of communication by electronic mail, the internet and data messages.[21] The ECT Act is a very wide piece of legislation and covers topics unrelated to electronic communications and transactions such as domain names, service providers' accountability and cyber inspectors.[22] It endeavours to bring certitude in spheres of law where there was legal ambivalence prior to August 2002 (e.g. 'click wrap' agreements).[23] Chapter VIII, deals with the Protection of Personal Information and only pertains to personal information acquired through electronic actions, requiring the data controller to freely subscribe to the principles contained in section 51.[24] Identification and authenticity of perpetrators in cyberspace remains problematic and represents a threat to both public and businesses.[25] The formation of an Accreditation Authority within the Department, allows for volitional accreditation of electronic signature in line with the minimal requirements.[26]

Chapter XIII is the first legislative provisions on cybercrime[27] in South Africa's practice of law.[28] The introduction of statutory transgressions relating to: Unauthorised access to, interception of or interference with data, ('hacking') and computer related extortion, fraud and forgery. The penalties include a fine or incarceration, the duration not exceeding one year in terms of section 86(4) or (5) or section 87 to a fine or incarceration the duration not exceeding five years.[29]

---

20 Act 25 of 2002.
21 Michalsons, 'Guide to the ECT Act in South Africa' (25 September 2008) <https://www.michalsons.com/blog/guide-to-the-ect-act/81> accessed 6 August 2020.
22 GN R458 in *GG* 23708 of 18 May 2007 (Electronic Communications and Transactions Act 25 of 2002 Chapter X, XI, XII).
23 SL Snail, 'An overview of South African e-consumer law in the context of the Electronic Communications and Transactions Act (part 2)' (2007) 15 JBL 54.
24 ECT Act, s 50.
25 Michalsons, 'Guide to the ECT Act in South Africa'.
26 ECT Act, Chapter VI – Authentication Service Providers.
27 ECT Act, ss 85-89.
28 Michalsons, 'Guide to the ECT Act in South Africa'.
29 ECT Act, s 89(2).

ECT Amendment Bill[30] has introduced schemes for the accreditation of authentication services and products to secure global electronic commerce, to prevent abuse of Information systems and cybercrime, amongst others, as well as the protection of South African domain names and to encourage the use of e-government services.[31] Many definitions have been amended, including, 'critical information' amended to 'critical data information',[32] for the protection of the national security and citizens; and 'critical information database', with 'critical information database infrastructure' for information to be in the electronic form within an electronic communications network, where it can be accessed, reproduced, distributed or extracted.[33]

3.2.3 South African Police Service Act (SAPSA)[34]

This makes it a criminal offence regarding computer access that is not authorised, belonging or in the control of the South African Police.[35] There is no restriction of access to any specific manner.[36] Access is not restricted to a specific manner and includes all forms of access,[37] and refers to access by 'whatever means'.[38] Subsection (2)[39] of the Act refers to the 'wilful' gaining of unauthorised access to any computer, or to any program or data held in such a computer, belonging to or under the control of the Service. The penalty on conviction is a fine or imprisonment for a period not exceeding two years.

Subsection (3)[40] of the Act refers to any person who wilfully performs a function who is not authorised to do so, shall be guilty of an offence with the penalty to a

---

30 Electronic Communications and Transactions Amendment Bill, 2012.
31 ECT Amendment Bill, 2012, Pre-amble.
32 ECT Amendment Bill, 2012 – para i.
33 ECT Amendment Bill, 2012 – para j.
34 Act 68 of 1995.
35 Section 71 of Act 68 of 1995.
36 Section 71 of Act 68 of 1995.
37 Sandra Mariana Maat, 'Cyber crime: a comparative law analysis' (LLM dissertation, University of South Africa 2004) Ch 3 at 9.
38 Section 71(1) of Act 68 of 1995.
39 Section 71(2) of Act 68 of 1995 'Any person who wilfully gains unauthorised access to any computer which belongs to or is under the control of the Service or to any program or data held in such a computer, or in a computer to which only certain or all members have restricted or unrestricted access in their capacity as members, shall be guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.'
40 'Any person who wilfully causes a computer which belongs to or is under the control of the Service or to which only certain or all members have restricted or unrestricted access

fine or to imprisonment for a period not exceeding two years. This subsection is not only applicable to all members that have restricted or unrestricted access, but also to those who cannot perform a function if not authorised.

Subsection 4, of the Act refers to any person who wilfully causes an unauthorised modification of the contents of any computer that impairs the operation of any computer or program or operating system, or prevents or hinders access, shall be guilty of an offence, and liable on conviction to a fine or to imprisonment for a period not exceeding five years. This subsection also refers to the word 'wilful', which emphasises the intent of a person. This may be an onus that is difficult to prove, if a person acted negligently.[41]

Subsection 5 of the Act deals with offences that were committed or took place outside the Republic of South Africa, shall be deemed to have been committed in the Republic, provided that the accused was in the Republic at the time of the offence, the computer was in the Republic at the time the accused committed the offence, and the accused was a South African citizen at the time of the commission of the offence.[42] The problem with this section is that the offences relating to unauthorised access or performing a function, or modification can be

---

in their capacity as members, to perform a function while such person is not authorised to cause such computer to perform such function, shall be guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.'

41 'Any person who wilfully performs an act which causes an unauthorised modification of the contents of any computer which belongs to or is under the control of the Service or to which only certain or all members have restricted or unrestricted access in their capacity as members with the intention to- (*a*) impair the operation of any computer or of any program in any computer or of the operating system of any computer or the reliability of data held in such computer; or (*b*) prevent or hinder access to any program or data held in any computer, shall be guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding five years.'

42 'Any act or event for which proof is required for a conviction of an offence in terms of this section which was committed or took place outside the Republic shall be deemed to have been committed or have taken place in the Republic: Provided that- (*a*) the accused was in the Republic at the time he or she performed the act or any part thereof by means of which he or she gained or attempted to gain unauthorised access to the computer, caused the computer to perform a function or modified or attempted to modify its contents-, (*b*) the computer, by means of or with regard to which the offence was committed, was in the Republic at the time the accused performed the act or any part thereof by means of which he or she gained or attempted to gain unauthorised access to it, caused it to perform a function or modified or attempted to modify its contents; or (*c*) the accused was a South African citizen at the time of the commission of the offence.'

committed outside the Republic by a foreign National. South Africa will then not have jurisdiction in respect of these specified offences, and it will the difficult to identify the perpetrator. These offences are specific to the SAPSA, and SAPS. However, section 71 of the Act will be deleted once the Cybercrimes Act is in full operation.

3.2.4 Correctional Services Act (CSA)[43]

Section 128[44] of the Correctional Services Act refers to unauthorised access to or modification of computer material. Access to a computer also refers to access by 'whatever means',[45] and includes access to any program or data that belongs to or is under the control of the Department or a custody official. Subsection (1)(*b*)[46] refers to the contents of a computer, which includes the physical components as well as any program or data contained in or stored. Subsection (1)(*c*)[47] refers to both temporary or permanent modification. Subsection (1)(*d*)[48] includes copying or downloading and subsection (*e*) is similar to the SAPSA,[49] regarding access which prohibited but includes situations where there is authorisation but no access to a particular program or where temporarily unauthorised to gain access.

Subsection (2)[50] refers to any person who intentionally, and not 'wilfully' as used in the SAPSA, gains prohibited access to a computer, which belongs to or in the

---

43 Act 111 of 1998.

44 Date of commencement of s 128: 19 February, 1999.

45 Section 128(1)(*a*) of Act 111 of 1998:
'(*a*) 'access to a computer' includes access by whatever means to any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under the control of the Department or a custody official.'

46 Section 128(1)(*b*) of Act 111 of 1998:
'(*b*) "contents of any computer" includes the physical components of any computer as well as any program or data contained in or stored as envisaged in paragraph (*a*)'.

47 Section 128(1)(*c*) ' "modifies" includes a temporary or permanent modification'.

48 Section 128(1)(*d*) ' "perform a function on a computer" includes copying or downloading; and s 128(1)(*e*) "unauthorised access" includes access by a person who is authorised to use the computer but unauthorised to gain access to a certain program or to certain data held in such computer or who is at the relevant time temporarily unauthorised to gain access to such computer, program or data.'

49 Act 68 of 1995.

50 'Any person who intentionally gains unauthorised access to any computer or to any program or data held in such a computer belonging to or under the control of the Department or Contractor, or in a computer to which correctional or custody officials have access in that capacity, is guilty of an offence and liable on conviction to a fine or, in

control of the agency, constitutes an offence where on conviction, a fine or imprisonment not exceeding twenty-four months can be imposed. Subsection (3)[51] refers to a person not authorised person who carries out any task on a computer has the same penalty as subsection 2.

Subsection (4)[52] refers to the intentional modification of the constituents of any computer that belongs or is under the control of the agency, which is similar to subsection (4) of the SAPSA[53] and its penalty provision. Subsection (5) of the Act,[54] is also similar to subsection (5) of the SAPSA. Section 128 of the Act is limited to computers that belong to or are under the control[55] of the Department of Correctional Services or a custody official. Section 128 of this Act will be deleted once the Cybercrimes Act 19 of 2020, is in operation.

3.2.5 National Prosecuting Authority Act (NPAA)[56]

The National Prosecuting Authority Act refers to unauthorised access,[57] which is specific to or modification of computer material.[58] The unauthorised access

---

default of payment, to incarceration for a period not exceeding two years or to such incarceration without the option of a fine or both.'

51 Section 128(3): 'Any unauthorised person who performs a function on a computer belonging to or under the control of the Department or a Contractor or to which correctional or custody officials have access, is guilty of an offence and liable on conviction to a fine or, in default of payment, to incarceration for a period not exceeding two years, or to such incarceration without the option of a fine or both.'

52 Section 128(4): 'Any person who intentionally modifies the contents of any computer belonging to or under the control of the Department or a Contractor or to which only correctional or custody officials have access in order to impair the operation of any computer or its operating or the reliability of data held in it or to prevent or hinder access to any program or data held in any computer, is guilty of an offence and liable on conviction to a fine or, in default of payment, to incarceration for a period not exceeding five years or to such incarceration without the option of a fine, or both.'

53 Section 71(4) of Act 68 of 1995.

54 Section 128(5): 'The courts of the Republic of South Africa have jurisdiction to try any person under this section whether such an offence was committed outside the Republic if— (*a*) the accused was in the Republic; (*b*) the computer concerned was in the Republic; or (*c*) the accused was a South African citizen.'

55 Maat, 'Cyber crime' 70.

56 Act 32 of 1998.

57 40A(1)(*d*): ' "unauthorised access" includes access by a person who is authorised to use the computer but is not authorised to gain access to a certain program or to certain data held in such computer or is unauthorised, at the time when the access is gained, to gain access to such computer, program or data.'

58 National Prosecuting Authority Act 32 of 1998, s 40A(2)(*c*).

includes access by a person who is authorised to use the computer but not authorised access to any data or program. Section 40A (1)(*c*) refers to modification,[59] which provision is similar to SAPSA[60] and CSA.[61] Section 40A(1)(*a*)[62] refers to access to a computer that belongs to or is under the control of the prosecuting authority, and included access by 'whatever means', which similar to the provisions of SAPSA[63] and CSA.[64] Section 40A(1)(*b*)[65] refers to the contents of any computer, which is similar to the provision of SAPSA.[66]

The penalty provision is a fine or a period of imprisonment not exceeding 25 years or both.[67] This penalty provision is much harsher than the ECT Act,[68] which imposes a penalty for the contraventions of 86(1), (2) or (3) to a fine or imprisonment for a period not exceeding 12 months, and the penalty for the contraventions of sections 86(4) or (5) or section 87 is a fine or imprisonment for a period not exceeding five years.

---

59 Section 40A(1)(*c*): 'modification includes both a modification of a temporary or permanent nature'.

60 Section 71(4) of Act 68 of 1995.

61 Section 128(1)(*b*) of Act 111 of 1998.

62 '40A Unauthorised access to or modification of computer material
(1) Without derogating from the generality of Subsection (2)-
(*a*) "access to a computer" includes access by whatever means to any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under the control of the prosecuting authority'.

63 Act 68 of 1995.

64 Act 111 of 1998.

65 Section 40A(1)(*b*) ' "contents of any computer" includes the physical components of any computer as well as any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under the control of the prosecuting authority'.

66 Section 71(4) of Act 68 of 1995.

67 Act 32 of 1998, s 41(4): 'Any person who is convicted of an offence referred to in Section 40A(2), shall be liable to a fine or to imprisonment for a period not exceeding 25 years or to both such fine and such imprisonment.'

68 Act 25 of 2002, s 89:
'(1) A person convicted of an offence referred to in Sections 37(3), 40(2), 58(2), 80(5). 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.
(2) A person convicted of an offence referred to in Section 86(4) or (5) or Section 87 is liable to a fine or imprisonment for a period not exceeding five years.'

Section 40A(2)(*a*) refers specifically to the gaining of unauthorised access of any computer or program under the control of the prosecuting authority.[69] The offences include performing a function, whilst not authorised to do so,[70] and an unauthorised modification which impairs or hinders the operation of a computer or the data.[71] Section 40A(3) is also similar to the provisions in SAPSA[72] and CSA,[73] which relates to an offence committed or that took place outside the Republic.[74] The NPA Act does not define the meaning of 'perform a function', which is concerning because of the penalty clause, whilst the CSA does. There does not appear to have been any reported cases with such a penalty imposed and the NPA website[75] does not provide a link on its prosecutions. Section 40A, and 41(4) of this Act will be deleted once the Cybercrimes Act 19 of 2020, is in operation.

---

69 Section 40A (2): 'Any person is guilty of an offence if he or she wilfully-
(*a*) gain, or allows or causes any other person to gain, unauthorised access to any computer which belongs to or is under the control of the prosecuting authority or to any program or data held in such a computer, or in a computer to which only certain or all members of the prosecuting authority have access in their capacity as members.'

70 Section 40A(2)(*b*): 'causes a computer which belongs to or is under the control of the prosecuting authority or to which only certain or all members of the National Prosecuting Authority Act 32 of 1998 prosecuting authority have access in their capacity as members, to perform a function while such person is not authorised to cause such computer to perform such function'.

71 Section 40A(2)(*c*): 'performs any act which causes an unauthorised modification of the contents of any computer which belongs to or is under the control of the prosecuting authority or to which only certain or all members of the prosecuting authority have access in their capacity as members with the intention to-
(i) impair the operation of any computer or of any program in any computer or of the operating system of any computer or the reliability of data held in such computer; or
(ii) prevent or hinder access to any program or data held in any computer.'

72 Section 71(5) of Act 68 of 1995.

73 Section 128(5) of Act 111 of 1998.

74 Section 40A(3): 'Any act or event for which proof is required for a conviction of an offence in terms of this section and which was committed or took place outside the Republic is deemed to have been committed or to have taken place in the Republic if-
(a) the accused was in the Republic at the time when he or she performed the act or any part thereof; or
(b) the computer, by means of which the act was done, or which was affected in a manner contemplated in Subsection (2) by the act, was in the Republic at the time when the accused performed the act or any part thereof; or
(c) the accused was a South African citizen or domiciled in the Republic at the time of the commission of the offence.'

75 National Prosecuting Authority of South Africa 'Justice in our society, so that people can in live in freedom and security' (2021) <https://www.npa.gov.za/> accessed 28 May 2021.

3.2.6 Financial Intelligence Centre Act (FICA)[76]

Section 66 of the FIC Act[77] is specific to computers that belong to or are under the control of the Centre. The maximum penalty provision can be 15 years imprisonment or to a fine not exceeding R10 000.00.[78] The FIC Act works in concert with the Prevention of Organised Crime Act[79] and the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 33 of 2004.[80] The purpose of the FIC Act is to establish a Financial Intelligence Centre and a Money Laundering Advisory Council in order to combat money laundering activities, and impose certain duties on institutions and persons who might be used for money laundering purposes.[81] Sections 65, 66 and 67, will be deleted once the Cybercrimes Act 19 0f 2020 is in operation.

3.2.7 Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)[82]

Section 2 of RICA refers to the prohibition of intentional interception of communication. Section 4(1) states that 'any person may intercept any communication if he or she is a party to the communication, unless the interception is for the purposes of committing an offence'.[83] The interception must not have the intention to commit an offence.[84] The admissibility and evidentiary weight of data messages is dealt with in section 15(3) of the ECT

---

76 Act 38 of 2001.

77 'Any person who, without authority to do so, wilfully causes a computer system that belongs to, or is under the control of, the Centre, or any application or data held in such a computer system, to be modified, destroyed, erased or the operation or reliability of such a computer system, application or data to be otherwise impaired, is guilty of an offence.'

78 Act 38 of 2001, s 68: '(1) A person convicted of an offence mentioned in this Chapter, other than an offence mentioned in Subsection (2), is liable to imprisonment for a period not exceeding 15 years or to a fine not exceeding R10 000 000. (2) A person convicted of an offence mentioned in Section 55, 61 or 62 is liable to imprisonment for a period not exceeding five years or to a fine not exceeding R1000 000.'

79 Act 121 of 1998.

80 Financial Intelligence Centre, 'Legislation' <https://www.fic.gov.za/Resources/Pages/Legis lationaspx> accessed 12 March 2021.

81 Act 38 of 2001, Preamble.

82 Act 70 of 2002.

83 Section 4(1), 'Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication. unless such communication is intercepted by such person for purposes of committing an offence.'

84 Corlett Manaka, 'Understanding the impact of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002' *Mondaq* [16 December 2010].

Act.[85] A huge blow for RICA, as the Constitutional Court handed down judgment on 4 February 2021, that RICA 'is unconstitutional to the extent that it fails to provide adequate safeguards to protect the right to privacy, as buttressed by the rights of access to courts, freedom of expression and the media, and legal privilege'.[86] The Judgement in *AmaBhungane Centre for Investigative Journalism*[87] confirmed the 'declaration of unconstitutionality', but only in respect of; the failure to come up with preventative measures to make sure that the designated Judge in terms of section1, is adequately autarchic; Rica also fails to notify the person of the surveillance and; fails to satisfactorily specify policies to make sure that obtaining of data in accordance with the interception of communications is handled licitly or with sufficient safeguards where the person under surveillance is a lawyer or journalist.[88]

---

85 '15(3) In assessing the evidentiary weight of data message, regard must be had to:
(*a*) the reliability of the manner in which the data message was generated, stored or communicated;
(*b*) the reliability of the manner in which the integrity of the data message was maintained;
(*c*) the manner in which its originator was identified; and
(*d*) any other relevant factor.'

86 Constitutional Court of South Africa, '*AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC 03' <https://www.concourt.org.za/index.php/judgement/383-amabhungane-centre-for-investi gative-journalism-npc-and-another-v-minister-of-justice-and-correctional-services-and-others-minister-of-police-v-amabhungane-centre-for-investigative-journalism-npc-and-others-cct278-19-cct279-19> accessed 8 March 2021.

87 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC 03 [6]-[7].

88 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* Case CCT278/19 & CCT279/19 [2021] ZACC 03 [6-7]:

'6. The declaration of unconstitutionality by the High Court is confirmed only to the extent that the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA) fails to—
(a) provide for safeguards to ensure that a Judge designated in terms of Section 1 is sufficiently independent;
(b) provide for notifying the subject of surveillance of the fact of her or his surveillance as soon as notification can be given without jeopardising the purpose of surveillance after surveillance has been terminated;
(c) adequately provide safeguards to address the fact that interception directions are sought and obtained ex parte;
(d) adequately prescribe procedures to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data; and
(e) provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist.

Cyber offences based on data obtained pursuant to the interception of communications, in respect of RICA, will impact directly on Extraditions, because of the unconstitutionality of these specific provisions. In the *AmaBhungane Centre for Investigative Journalism*, the court said that there must be adequate procedures, for examining, copying, sharing, sorting through, using, storing or destroying the data.[89] In a majority judgment penned by 'Madlanga J (Khampepe J, Majiedt J, Mathopo AJ, Mhlantla J, Theron J, Tshiqi J and Victor AJ concurring)', the Constitutional Court held that interception and surveillance of an individual's communications under RICA is a highly invasive violation of privacy, and thus infringes section 14 of the Constitution.[90]

3.3 Cybercrimes Act and its criticisms[91]

3.3.1 Freedom of expression

Chapter 2 of the Cybercrimes Act seeks to regulate 'Malicious Communications'.[92] The Right2Know (R2K) Campaign argues that protecting online freedom of expression is challenging in 'an environment where patriarchy, racism, hatred and toxicity thrive'.[93] These legal provisions are open to abuse, mainly on how the Act defines what messages are considered harmful.[94] A petition was signed with the demand to withdraw the Cybercrime Bill and its proposed regulations on 'malicious communications', because of the

---

7. The declaration of unconstitutionality in paragraph 6 takes effect from the date of this judgment and is suspended for 36 months to afford Parliament an opportunity to cure the defect causing the invalidity.'

89 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC 03 [6(*d*)].

90 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* Case CCT278/19 & CCT279/19 [2021] ZACC 03 [188].

91 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill' (8 April 2017) <https://www.R2k.Org.Za/2017/08/11/R2k-Submission-on-the-Cybercrimes-Bill-2017> accessed 23 December 2020.

92 Cybercrimes and Cybersecurity Bill Republic of South Africa (published in *GG* 40487 of 9 December 2016) (hereinafter referred to the Cybercrimes Bill 2017), Part II.

93 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.

94 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.

censorship on social media.[95] The erstwhile State Security Minister, David Mahlobo had stated that government was considering regulations for social media, with the aim of addressing 'fake news' and 'false narratives'.[96] The argument is that the Act will make 'malicious communications' a crime, including anything which is 'inherently false', but the question is: who decides what is false or not?[97] Millions of South Africans come to social media platforms that access and share information freely, with the right to exercise freedom of expression as a vital part of democracy.[98]

The argument is that the Minister of State Security cannot be allocated unfettered power to decide what news is 'fake' and 'false', since democracy is about citizens exercising their own judgement and decisions.[99] The further argument was that across the world,[100] governments tried to regulate social media in the name of national security, which has led directly to Internet censorship and a clampdown on freedom of expression, and South Africa was not going to be allowed to go the same route.[101]

3.3.2 Inciting or threatening violence and property damage

Section 14[102] makes it a criminal offence for any person who discloses a data message for the purpose of inciting or causing any damage to property or violence to a person or a group of persons. Sections 15(*a*)[103] and 15(*b*)[104] of the Act[105] would render it a criminal offence to send or resend a message that:

---

95 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.

96 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.

97 Right2Know Campaign, 'Hands Off Social Media' <https://awethu.amandla.mobi/petitions/handsoffoursocialmedia> accessed 23 December 2020.

98 Right2Know Campaign, 'Hands Off Social Media'.

99 Right2Know Campaign, 'Hands Off Social Media'; Right2Know Admin, 'State security: hands off the internet! No to spooks regulating social media' (8 April 2019) <http://www.r2k.org.za/2017/03/07/state-security-hands-off-the-internet-no-to-spooks-regulating-social-media/> accessed 23 December 2020.

100 Right2Know Campaign, 'Hands Off Social Media'. These include Brazil, China, Ethiopia and Zimbabwe.

101 Right2Know Campaign, 'Hands Off Social Media'.

102 Section 14 of the Cybercrimes Bill [B 6D—2017] 'Any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite— (*a*) the causing of any damage to property belonging to; or (*b*) violence against, a person or a group of persons, is guilty of an offence.'

103 Section 15 of the Cybercrimes Bill [B 6D—2017]: 'A person commits an offence if they, by means of an electronic communications service, unlawfully and intentionally discloses a

> Threatens a person with violence or property damage;
>
> Threatens violence or property damage against a group of people, or any person who is associated with a group of people.

The R2K Campaign argued that in principle, these laws should be rejected forthright. Laws prohibiting freedom of speech could be materially harmful, and criminal penalties should be implemented in proportion with the harm that has been done.[106]

3.3.3 Orders to protect complainants from the harmful effect of malicious communications

Part VI of the Act refers to protection orders. The R2K Campaign argues that this needs to be addressed in the Protection from Harassment Act,[107] including harassment, through the Internet and telecommunications platforms.[108] The answer recites in greater public awareness with better enforcement by the justice system, as well as additional criminal penalties are not the answer imposed through the Cybercrimes Act.[109]

3.3.4 Freedom from surveillance

In recent times, the Right2Know Campaign has argued also that section 40 (previously known as section 38) of the Cybercrimes Act claims creation of several RICA reforms. The most debatable issue has been that surveillance was used for targeting investigative journalists, unionists, political activists, and

---

data message, which— (*a*) threatens a person with— (i) damage to property belonging to that person or a related person; or (ii) violence against that person or a related person.'

104 Section 15(*b*) of the Cybercrimes Bill 2017: 'threatens a group of persons or any person forming part of, or associated with, that group of persons with— (i) damage to property belonging to that group of persons or any person forming part of, or associated with, that group of persons; or (ii) violence against the group of persons or any person forming part of, or associated with, that group of persons'.

105 Cybercrimes Bill 2017.

106 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill' (8 April 2017) <https://www.R2k.Org.Za/2017/08/11/R2k-Submission-on-the-Cybercrimes-Bill-2017> accessed 23 December 2020.

107 Act 17 of 2011, s 2.

108 Cybercrimes Act 2017, s 20.

109 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.

interferes in South Africa's politics and public life.[110] The abuse is made possible on the basis of RICA's lack of transparency, or adequate safeguards. It was argued that the most potent mass surveillance systems were not regulated by Rica.[111] The demand was that the State should drop sim card registrations, end the mass storage of data and strengthen judicial protection against surveillances.[112] Section 40(1)[113] of the Cybercrimes Act states that the interception as defined in section 1 of RICA should occur as directed by a designated judge in terms of section 16(4)[114] or section 18(3).[115] The findings by the UN Human Rights Committee[116] expressed concerns with the right to privacy and the interception of private communications; the comparatively low threshold for the conduct of surveillance and the relatively weak safeguards, remedies and oversight against unlawful interference with the right to privacy contained in (RICA).[117] The Committee was further concerned with reports of illegal surveillance and the mass communications' interception. In this regard, the State should desist from engaging in mass surveillance in the absence of judicial authorisation, and that interceptions should be carried out under judicial

---

110 Right2Know Campaign, 'R2K protests against Rica surveillance' News24 (26 April 2016) <https://www.news24.com/News24/right2know-protests-against-rica-surveillance-20160426> accessed 23 December 2020.

111 Right2Know Campaign, 'R2K protests against Rica surveillance'.

112 Right2Know Campaign, 'R2K protests against Rica surveillance'.

113 Section 40(1) of the Cybercrimes Act: 'the interception of an indirect communication as defined in Section 1 of the Regulation of Interception of Communications and Provision of Communication- related Information Act, 2002, must take place in terms of a direction issued in terms of Section 16(4) or 18(3) of that Act and must, subject to Subsection (4), be dealt with further in the manner provided for in that Act.'

114 Section 14(4) of RICA: 'Notwithstanding Section 2 or anything to the contrary in any other law contained a designated judge may upon an application made to him or her in terms of subsection (1) issue an interception direction.'

115 Section 18(3) of RICA: 'Notwithstanding Sections 2 and 12. or anything to the contrary in any other law contained. a designated judge may upon an application made to him or her in terms of -

(*a*) Subsection (1) and subject to Sections 16(5), (6) and (7), 17(4), (5) and (6) and l9(4), (5) and (6). issue the combination of directions applied for: or

(*b*) Subsection (2) and subject to Section 17(4), (5) and (6) issue a real-time communication-related direction to supplement that interception direction:
Provided that a real-time communication-related direction issued under these 25 paragraphs expires when the period or extended period for which the interception direction concerned has been issued, lapses.'

116 United Nations (UN) Human Rights Committee 'International Covenant on Civil and Political Rights' (27 April 2016) 148 <https://www.justice.gov.za/ilr/docs/2016-ICCPR-SA-ConludingObservations-April2016.pdf> accessed 30 December 2020. The Committee considered the initial report of South Africa (CCPR/C/ZAF/1) at its 3234th and 3235th meetings (CCPR/C/SR. 3234 and 3235), held on 7 and 8 March 2016. At its 3258th meeting, held on 23 March 2016, it adopted the present concluding observations.

117 UN, 'International Covenant on Civil and Political Rights' para 42.

supervision.[118] The report also stated the need for a transparent surveillance policy and the expeditious establishment of independent mechanisms for oversight.[119]

RICA is blamed for lack of transparency and the attendant poor oversight that has infringed on the privacy of millions of citizens.[120] The R2K Campaign commented on the Bill's modest changes to RICA. The first reform relates to 'Storage of users' and Internet browsing information relating to a person's communication that had to be stored in terms of RICA for periods of up to five years,[121] which was never operationalised. In the same breath, argued that such practice was unconstitutional from a human rights perspective.[122] The second reform relates to closing the gap of a loophole in section 205 of the Criminal Procedure Act,[123] regarding a duplicate action for the access of a person's private and confidential information notwithstanding the fact that it is under the aegis of a RICA judge.[124]

The R2K Campaign also requested that urgent changes were required to protect citizens' privacy. The point of concern the Cybercrimes' Act failure to take other cogent steps for the correction of the many loopholes in RICA, as well as injurious provisions the State to spying on its own citizens and employing surveillance as a mechanism for repression.[125]

Another criticism of the Act relates to section 33(1), concerning the search, seizure of, or access to an article on the arrest of a person. This section states that:

> A police official may without a warrant, as contemplated in section 40 of the Criminal Procedure Act 51, 1977, arrest any person (*a*) who commits any offence in terms of Part I or Part II of Chapter 2 in their presence; (*b*) whom

---

118 UN, 'International Covenant on Civil and Political Rights' para 43.
119 UN, International Covenant on Civil and Political Rights' para 43.
120 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
121 Section 30(2)(*a*)(iii) 'type of communication-related information which must be stored in terms of Subsection (1)(*b*) and the period for which such information must be stored which period may, subject to Subsection (8) not be less than three years and not more than five years from the date of the transmission of the indirect communication to which that communication-related information relates'.
122 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
123 Act 51 of 1977.
124 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
125 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.

> they reasonably suspect of having committed any offence in terms of Part I and Part II of Chapter 2.

There is no reference to a citizen's arrest referred to in section 42 of the CPA, in terms of which:

> Arrest by private person without warrant, 42(1). Any private person may without warrant arrest any person –
>
> (*a*) who commits or attempts to commit in his presence or whom he reasonably suspects of having committed an offence referred to in Schedule 1;
>
> (*b*) whom he reasonably believes to have committed any offence and to be escaping from and to be freshly pursued by a person whom such private person reasonably believes to have authority to arrest that person for that offence.

This means that an investigator or a private person cannot effect a citizen's arrest. The genuine capacity to secure cyberspace[126] and fight cybercrime will not be successful if such initiatives are entrusted and making more secure will not be successful if it is entrusted solely to the police. The R2K Campaign stated that: 'what the Cybercrimes Act doesn't do; can't do, detect, solve cybercrimes and the expertise inside the State to create better defences against cybercrime'. Such oversight of excluding section 42 of the CPA appears to be fatal.

Further analysis reveals that the Act refers to theft of incorporeal property in terms of section 12, which states: 'The common law offence of theft must be interpreted so as not to exclude the theft of incorporeal property.'

Section 36 of the General Law Amendment Act[127] states:

> Any person who is found in possession of any goods, other than stock or produce as defined in section thirteen of the possession of Stock Theft Act, 1923 (Act No. 26 of 1923), in regard to which goods there is reasonable suspicion that they have been stolen and is unable to give a satisfactory account of such possession, shall be guilty of an offence and liable on conviction to the penalties which may be imposed on a conviction of theft.

An investigator, under the Cybercrimes Act would not be able to request a person for an explanation, to give a satisfactory account of such possession

---

126 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
127 Act 62 of 1955.

where there is reasonable suspicion that goods have been stolen. In *Doma v S*,[128] it was stated that:

> Section 36 is a quintessential example of what might be called a 'policeman's crime' to afford an alert police officer the right to lawfully stop and interrogate a person, who is honestly and reasonably suspected by the police officer of wrongdoing.[129]

The act of 'finding' has to be done by the police.[130] This Act then provides an investigator or a citizen to effect an arrest or question a person in possession of goods where reasonable suspicion exists that goods were stolen. It is a concern that the police will not cope and new complex or less effective legislation will only aggravate the serious capacity issues already faced in respect of cybercrime.[131]

The concern is that the Act relates only to cybercrimes, whilst cybersecurity is severed. The cybersecurity for government agencies ensures the State is privy to what is happening on the Internet, and has the ability to intervene when someone is behaving unlawfully.[132] We each have the right to cybersecurity, and transgression of our cybersecurity could become a concomitant violation of our fundamental human right.[133] Cybersecurity law is enjoined to protect people on three levels: protection on personal data, protection of devices and protection of networks that are being used. There is an on-going measure of threats to our information from private companies, criminals and State agencies, both foreign and domestic.[134]

The realistic effect of the Cybercrimes Act on all individuals and organisations is considerable. Unfortunately, all forms of negativity attendance to our cybersecurity have not been resolved. The enforcement of law is inadvertently becoming an infraction to our freedom by criminalising everyday life, affecting everyone,[135] who processes data or uses a computer, including individuals,

---

128 *Doma v S* (2012/A447) [2013] ZAGPJHC 116 (21 May 2013) (hereinafter referred to the *Doma* case).
129 *Doma* case [36].
130 Snyman, *Criminal Law* 525.
131 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
132 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
133 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
134 Right2Know Campaign, 'R2K submission on the Cybercrimes Bill'.
135 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read'.

journalists, organisations, banks and many others who may probably be committing many daily offences.[136]

3.4 South Africa's Protection of Personal Information Act (POPIA)[137]

The POPI Act seeks to 'regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy',[138] in accordance with section 14 of the Constitution.[139] Laws pursuant to data privacy are measures intended to protect data subjects from possible harm emanating from the manual or computerised 'processing of their personal information by data vendors or controllers'.[140] Globally, the transfer and collection of personal information has become an everyday occurrence.[141] Sometimes, personal information is collected clandestinely through technological infringements about which the data subject is unaware; for example, the use of cookies and Cloud computing.[142] This implies that stored information can no longer be linked to a physical place, and the exclusive control over the personal data does not always have sufficient information about the manner of data processing, by whom it is done and where the processing occurs,[143] which would be difficult to criminally prosecute. The ECT Act absolves itself from imposing legally binding obligations on data controllers,[144] which is a major deficiency. However, the POPI Act imposes duties on information officers[145] which assist in combating many challenges presented by identity theft crimes.[146]

POPI is based on a European data protection law that has been in force in the EU since 1995, and the Organisation for Economic Co-operation and

---

136 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read'.
137 Act 4 of 2013.
138 POPI Act 4 of 2013, Preamble.
139 Constitution of the Republic of South Africa, 1996.
140 Basdeo, 'Criminal and Procedural Legal Challenges' 369.
141 Basdeo, 'Criminal and Procedural Legal Challenges' 364.
142 Basdeo, 'Criminal and Procedural Legal Challenges' 365. 'A cloud computing services provider can offer various services such as data storage space as well as software applications to multiple customers on demand. This implies that instead of storing data and software on a user's hard drive, it is now stored on various servers which could be located anywhere in the world, and accessed when needed, via the internet.'
143 Basdeo, 'Criminal and Procedural Legal Challenges'.
144 ECT Act, s 51.
145 POPI Act, s 55.
146 Basdeo, 'Criminal and Procedural Legal Challenges' 375.

Development, (OECD), principles,[147] which regulates all aspect pertaining to the processing of personal information, from its collection to its destruction.[148] The EU's Directive,[149] imposed a prohibition on the transfer of personal data to non-member countries that did not ensure an adequate level of protection when personal data of their citizens are processed.

The General Data Protection Regulation (GDPR) subsequently replaced the Data Protection Directive because firstly; there was 'legal fragmentation' in the manner of its implementation by different States. Secondly, the Directive no longer provided legal certainty[150] owing to globalisation and the rapid development of technology. South Africa eventually implemented part of the POPI Act on 1 July 2020.[151] In this regard, the POPI Act could be viewed as an omnibus data protection prescript that conforms to the former benchmark for data protection laws worldwide,[152] (the 1995 EU Data Protection Directive).[153]

In 2016, the EU adopted the GDPR[154] that replaced the 1995 Directive effective from May 2018.[155] Roos analysed the selective provisions under the GDPR and compared them with provisions of the POPI Act, in order to establish whether

---

147 Basdeo, 'Criminal and Procedural Legal Challenges' 375.

148 Pamela Stein, 'South Africa's EU-Style Data Protection Law' (2012) 12 Without Prejudice 48.

149 Directive 95/46/EC of the European Parliament and of 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 Art (56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations; (57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited; <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046> (No longer in force, date of end of validity: 24 May 2018) accessed 8 March 2021.

150 Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and Its Implications for South African Data Privacy Law : An Evaluation of Selected' (2020) CILSA 53.

151 Parliament, 'Justice Committee wants urgent implementation of full POPIA' (12 May 2020) <https://www.parliament.gov.za/press-releases/justice-committee-wants-urgent-implemen tation-full-popia> accessed 25 May 2020.

152 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 4.

153 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <http://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 8 March 2021.

154 Directive 95/46/EC.

155 Directive 95/46/EC.

the changes in the EU position would require amendments to the POPI Act insofar as meeting the minimum standards for data protection set by the EU Regulation.[156] The comparison of the GDPR and the POPI Act with regard to the content of specific concepts and the legal bases for lawful processing. Roos, concluded that that the content of concepts such as personal data or information, the processing of personal information, data controller, data processor, recipient, and special categories of personal data found in the POPI Act is equivalent to the content of those concepts in the GDPR.[157]

There were differences with the grounds for lawful processing of information, suggesting that the POPI Act should be amended for its compliant with the standard set in the GDPR, before approaching the EU for such a declaration.

3.5 Conclusion

The different pieces of legislation that refer to unauthorised access are limited to computers that are under their control. The Cybercrime Act 19 of 2020, has eliminated all references to cybersecurity,[158] and the Cybercrimes Act still awaits the proclamation in the Government Gazette. It has been recommended[159] that the POPI Act should be amended to comply with the standards set in the GDPR where offences cannot satisfy the double criminality principle, coupled with the lack of enforcement. The role of technology has significantly altered the manner in which people conduct their business and communicate.[160]

South Africa is still lagging behind in comparison with advanced economies in terms of cybersecurity legislation, coordination of government, engaging with business and citizens, and in respect of supplying skilled labour.[161] These delays translate into deficiency in comparison with experiences of fast growing

---

156 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 6.
157 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31.
158 Michalsons, 'Cybercrimes Act in South Africa: Overview and Read'.
159 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31.
160 Fatima Ameer-Mia and Lee Shacksnovis, 'Cybercrimes Bill – A positive step towards the regulation of cybercrimes in South Africa' (*Technology and Sourcing*, 13 February 2019) 4 <https://www.cliffedekkerhofmeyr.com/export/sites/cdh/en/news/publications/2019/technology/downloads/Technology-Sourcing-Alert-13-February-2019.pdf> accessed 6 June 2020.
161 Sutherland, 'Governance of cybersecurity' 83.

economies, and the concomitant improvements in their policy implementation.[162] Chapter XII of the ECT Act provides for the creation of a Cyber Inspectorate, with powers to search, inspect and seize content. These powers are meant to complement the initiatives by other law enforcement agencies, and to directly service to public and businesses. Additionally, no implementation regulations were promulgated, neither were Cyber Inspectors appointed, and no Chapter XIII offenses were ever prosecuted.[163] Similarly, prosecutions for the crime of criminal defamations were rare; despite people being defamed daily, yet no-one one has ever been convicted of this crime for decades.[164] It is hoped that the Cybercrimes Act will not be another ivory tower piece of legislation with slow implementation or where nothing is done.

The Cybercrimes Act creates new cybercrime offences, namely: unlawful access,[165] and interception of data,[166] unlawful software related offenses, acts in respect of software,[167] unlawful interference with a computer program or data;[168] illegal interference with a computer data storage medium or computer system,[169] unlawfully acquiring, possessing, providing, receiving or using password, accessing a code or similar data or device,[170] cyber fraud,[171] cyber forgery and uttering,[172] cyber extortion,[173] aggravated transgressions;[174] as well as theft of incorporeal property.[175] The Cybercrimes Act affords the investigator[176] wide ranging authority to search, investigate, access, and seize[177] anything that is materially related to a computer in question.

---

162 Sutherland, 'Governance of cybersecurity' 83.
163 Sutherland, 'Governance of cybersecurity' 90.
164 In *Hoho v The State* (493/05) [2008] ZASCA 98 (17 September 2008) the Supreme Court of Appeal held that the crime was not abrogated by disuse. See also Bregmans 'Criminal Defamation' (26 June 2019) <https://www.bregmans.co.za/criminal-defamation/> accessed 10 March 2021.
165 Cybercrimes Act 19 of 2020, s 2.
166 Cybercrimes Act 19 of 2020, s 3.
167 Cybercrimes Act 19 of 2020, s 4.
168 Cybercrimes Act 19 of 2020, s 5.
169 Cybercrimes Act 19 of 2020, s 6.
170 Cybercrimes Act 19 of 2020, s 7.
171 Cybercrimes Act 19 of 2020, s 8.
172 Cybercrimes Act 19 of 2020, s 9.
173 Cybercrimes Act 19 of 2020, s 10.
174 Cybercrimes Act 19 of 2020, s 11.
175 Cybercrimes Act 19 of 2020, s 12.
176 Cybercrimes Act 19 of 2020, s 25 – definitions.
177 Cybercrimes Act 19 of 2020, s 25 – definitions.

The National Commissioner is required to designate or establish an office of the South African Police Service (SAPS) within its existing structures which is to be known as the designated Point of Contact[178] and must ensure the provision for immediate assistance for investigations or proceedings concerning the commission of an offence.[179] This is potentially problematic insofar as the establishment of the cybercrime units with the 'compounded issues of budget cuts, reduced overtime pay, the changing nature of the crime, increasing levels of crime, lack of social support for the police, continual breakdown and creation of specialized units, and low morale all contribute to increased risk of burnout'.[180] Additionally, there is currently a shift from the traditional method of policing to community policing.[181] To this effect, Ntshengedzeni intimates that the proper implementation of community solution to building partnerships between SAPS and local communities.[182] An understaffed police service is one of the reasons for community policing mainly, and yet the police are still required to render immediate assistance in cybercrime cases, which poses a further challenge but raises criticisms.

The problems of laws which are not enforced have no consequences. The enforcement of law is not only to deal with individual violators but also to remind society of the legality of civilization.[183] 'One protester who disrupts a speech is not the problem, but if unpunished, he green-lights hundreds more like him'.[184] Similarly, the extradition of an individual who has committed cybercrime offences in a foreign jurisdiction, will most probably succeed, in him raising the defence of double criminality, if no offence exists, or not enforced at the time that the request was made at the requested state.

---

178 Cybercrimes Act 19 of 2020, s 52(1)(*a*).

179 Cybercrimes Act 19 of 2020, s 52(3)(*a*).

180 Grainne Perkins, 'Shedding light on the hidden epidemic of police suicide in South Africa' (3 February 2016) <https://theconversation.com/shedding-light-on-the-hidden-epidemic-of-police-suicide-in-south-africa-53318> accessed 31 December 2020 50.

181 Ntshengedzeni Albert Netshitangani, 'An evaluation of the implementation of community policing in Westonaria' (MA dissertation, University of South Africa 2018) 1.

182 Netshitangani, 'An evaluation of the implementation of community policing' 1.

183 Victor Davis Hanson, 'When laws are not enforced, anarchy follows' *Tribune News Service* (3 November 2018).

184 Hanson, 'When laws are not enforced, anarchy follows'.

Roos made the following recommendations which would elevate South Africa to international standards:[185]

Firstly, this should be a requirement for the data subject gives consent by means of a clear affirmative action.[186]

Secondly: In the event of consent the grounds for the processing special categories of personal information, should be a requirement for the data subject explicitly give such consent.[187]

Thirdly: In the case of processing of an obligation which is imposed by law on the party responsible, it should be a requirement for the processing of data as a necessary requirement.[188]

---

185 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31.
'(1) In the case of consent as a ground for processing personal information in general, it should be required that the data subject gives consent by means of a clear affirmative action.
(2) In the case of consent as a ground for processing special categories of personal information, it should be required that the data subject explicitly gives such consent.
(3) In the case of processing that complies with an obligation imposed by law on the responsible party or processing that protects a legitimate interest of the data subject, it should be required that the processing is necessary to fulfil those purposes.
(4) In the case of processing personal information to protect the interests of the data subject, it should be required that the interests that are to be protected are vital and it must be provided that public authorities may not use this ground as a basis for processing personal information but must instead have another legal basis provided by the legislator.
(5) Where processing of personal information is allowed in order to carry out the obligations of the data controller or to exercise the rights of the data subject in the field of employment, and social security and social protection law; or where a foundation, association or another not-for-profit body with a political, philosophical, religious or trade union aim is allowed to process the special personal information of its members; or where processing of special personal information is allowed in the medical field; and where processing for archiving, scientific or historical research purposes, or statistical purposes is allowed, such processing should be authorised by a law, an agreement or a contract.
(6) Regarding the processing of information relating to criminal convictions, it would be advisable to follow the example set by the GDPR and to spell out that only an official authority may keep a comprehensive register of criminal convictions.
(7) Where the processing of special categories of personal information is allowed on the basis that it is in the public interest, it should be a requirement that the public interest is substantial and that the processing takes place on the basis of a law. Such a law should be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

186 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31; see also Hanson, 'When laws are not enforced, anarchy follows'.

187 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31; see also Hanson, 'When laws are not enforced, anarchy follows'.

Fourthly: In the case of processing to protect the interests of the data subject, it should be a requirement that the interests protected are vital. Public authorities may not have the same ground as a basis for processing personal information, but should instead, have another legal basis provided by the legislator.[189]

Fifthly: Where processing is allowed for purposes of carrying out the obligations or concerning the rights of the data subject in the field of 'employment, social security and social protection law; or where a foundation, association or another not-for-profit body with a political, philosophical, religious or trade union is allowed to process the special personal information of its members; or where processing of special personal information is allowed in the medical field; and where processing for archiving, scientific or historical research purposes, or statistical purposes is allowed',[190] it should be a required that such processing should be authorised by a specific law, agreement or contractually.

Sixth: Regarding criminal transgressions, it would be advisable to follow the example by the GDPR pronouncing that only official authorised persons may keep criminal convictions.[191]

Seventh: Special categories of personal information processed on the basis of the public interest, there should be a requirement substantial and that the basis of the basis of the processing basis is according to law. Such law should be commensurate to its intended objective, valuing the ethos of the right to protect data, furnishing appropriate specified means to protect the basic rights of the data subject.[192]

---

188 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31; see also Hanson, 'When laws are not enforced, anarchy follows'.

189 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31; see also Hanson, 'When laws are not enforced, anarchy follows'.

190 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 31; see also Hanson, 'When laws are not enforced, anarchy follows'.

191 Roos, 'The European Union's General Data Protection Regulation (GDPR)'; see also Hanson, 'When laws are not enforced, anarchy follows'.

192 Roos, 'The European Union's General Data Protection Regulation (GDPR)'; see also Hanson, 'When laws are not enforced, anarchy follows'.

Roos further recommends[193] that the legislature should also consider introducing the following provisions found in the GDPR:

- The processing of special information categories be a requirement in order to protect the interest of the public in the sphere of public health, especially against serious cross-border risks to health such as communicable diseases, which must be prevented and controlled. There must be high quality standards of quality and healthcare safe, as well as medicinal products or medical devices must be ensured. The basis of processing must be done on a law providing for appropriate specific measure that safeguard the rights and freedoms of the data subject, especially professional confidentiality.
- The legislature should also consider situations in which data subjects should not be allowed to give consent to the processing of special personal information.

Roos stated further that there were other provisions relating to the 'data-protection principles, data subject rights, restrictions on onward transfer and the procedural and enforcement mechanisms' which should also be evaluated before a definitive answer can be provided of whether or not the POPI Act fulfils the benchmark requirements by the GDPR.[194] The EU Directive was repealed in 2018, and its POPI Act variant is now fully implemented since July 2021. The delay in the implementation of POPPI was largely based on a law that is now repealed should now be comparable to the GDPR, but it is concerning that this may be insufficient. POPI cannot only be compared to the GDPR, because the UK-DPA is a massive piece of legislation that received Royal Assent on 23 May 2018,[195] and supplements the GDPR.

While POPI's processing of personal information will operationalise the right to privacy, it may fail on international standards and harmonisation. This is also another concern for South Africa, with part of the RICA Act being declared unconstitutional, to the degree it lacks in providing adequate safeguards that protect the right to privacy.[196] This raises the further apprehension that some of South Africa's legislation does not accord with international standards created

---

193 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 32.
194 Roos, 'The European Union's General Data Protection Regulation (GDPR)' 32.
195 UK Public General Acts 2018 c.12 (Data Protection Act) (DPA).
196 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC 03 [6]-[7].

for opportunity for criminals who commit offences, without fear[197] of prosecution or extradition.

It is evident that for extradition to be effective, crimes in different jurisdictions need to be materially similar. This is a question that is addressed in the next Chapter when cyber legislation in the United Kingdom and the United States of America are discussed.

[197] Mujuzi, 'The South African International Co-Operation in Criminal Matters Act' 351.

Chapter 4: The United Kingdom and the United States cyber laws, and the European arrest warrant

4.1 Introduction

There is no single security cyber law in the UK, but many comprehensive cybersecurity laws are to be found. These are statute-based laws,[1] include: the Computer Misuse Act 1990 (CMA), the Investigatory Powers Act 2016 (IPA), the Data Protection Act 2018 (DPA), and the Network and Information Systems Regulations 2018 (NISR), the Fraud Act 2006 (FA), the Theft Act 1978, the Proceeds of Crime Act 2002 (PCA), Copyright, Designs and Patents Act 1988. The IPA, the Police Act 1997 and the Intelligence Services Act 1994,[2] are intended to protect the interests of national security. Furthermore, these are applied in prosecutions of cyber-attacks in the UK to also protect the financial security of citizens.[3]

Due to a plethora of laws in the UK, including the cyber and cybersecurity laws adversely impact on extraditions between States, with the double criminality requirement between States, the European Arrest Warrant (EAW),[4] was introduced in 2002. The main objective of the European Union was to simplify, expedite procedures, and contribute to optimally uniform application.[5] The transfer procedure for persons differs fundamentally from the conventional extradition procedures by eliminating the division of tasks between the two

---

1 Julian Hayes and Michael Drury, 'Cybersecurity in United Kingdom (England & Wales)' (*Lexology,* 23 December 2019) <www.lexology.com›library›detail›g=09262dc8-60...> accessed 21 March 2021.

2 Hayes and Drury, 'Cybersecurity in United Kingdom'.

3 Rahul Sharma, 'Legislation Related to Cyber-Crimes in United Kingdom' (December 2020) <https://www.researchgate.net/publication/347439774_Legislation_Related_to_Cyber_Crimes_in_United_Kingdomouth.Ac.Uk> accessed 15 January 2021.

4 Council of the European Union, 'Council Framework Decision' (2002/584/JHA) (13 June 2002) on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision; International Law & Order 1; Official Journal of the European Communities <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584> accessed 30 August 2020.

5 Gheorghe Pinteală, 'Legal aspects of the European arrest warrant' Quaestus Multi-disciplinary Research Journal 183 <https://www.quaestus.ro/wp-content/uploads/2012/03/pinteala2.pdf> accessed 13 February 2021.

parties, that is, the Justice Ministry and the court.[6] The decision on the EAW does not adequately allocate automatic extradition, but allows Member States the opportunity to provide the dissemination of the European arrest warrant on the material aspects.[7]

The UK and the United States (US), can be regarded as epitomising the common law system, and case law is vitally important in both of these jurisdictions.[8] The UK and the US are parties[9] to the Convention on Cybercrime.[10] The capacity of the US in the use of existing criminal law in the regulation of cybercrime, allocated it as a forerunner and to promulgating new laws dating back to the 1970s.[11] It is admirable that the US, with the Computer Fraud and Abuse Act[12] (CFAA), has somewhat struck the balance between online freedom and control over cyberspace, with the evolution of the CFAA.[13] However there are also some prevalent challenges for instance, the National Association of Criminal Defence Lawyers (NADCL) contend that generalising the CFAA will require that adequate notice be given to users of the internet, as to the type of conduct that is disallowed, whilst it concomitantly fails to give perspicuous rules to manage legal enforcement.[14]

4.2 Legislation regarding the CMA, IPA, DPA, NISR and FA

4.2.1 Computer Misuse Act of 1990 (CMA)

This Act is the prime regulation considered for the penalisation of cybersecurity related crimes. The Act makes provision for securing computer material against

---

6 Pinteală, 'Legal aspects of the European arrest warrant'.
7 Council of the European Union, 'Council Framework Decision' arts 4 and 5.
8 Wang, *A Comparative Study of Cybercrime in Criminal Law* 27.
9 Council of Europe, Convention on Cybercrime: Chart of Signatures and Ratification of Treaty 185 (23 November 2001) <https://www.coe.int/en/web/conventions/full-list/-/conven-tions/treaty/185/signatures> accessed 15 May 2021.
10 European Convention on Cybercrime, 'Budapest, 23.X1.2001 European Treaty Series - No 185' <https://Rm.Coe.Int/1680064587> accessed 29 April 2020.
11 Wang, *A Comparative Study of Cybercrime in Criminal Law* 99.
12 Computer Fraud and Abuse Act 1984, Coded as 18 U.S.C. § 1030, which is changed into the Computer Fraud and Abuse Act in 1986.
13 Wang, *A Comparative Study of Cybercrime in Criminal Law*.
14 NACDL, 'CFAA Background' (10 March 2020) <https://www.nacdl.org/Content/CFAABackground> accessed 15 May 2021.

unauthorised access or modification; and for connected purposes.[15] Section 1 of CMA, refers to access that is not authorised computer material. The Act renders it an offence for a person to perform a computer function post to seek access to any program, and the intent by a person directed at any particular data or program.[16]

The Computer Misuse Act 1990 establishes three clearly defined criminal offenses, namely[17] 'the unauthorized access to computers, which includes the illicit copying of software,[18] intentional unauthorized access to commit further offenses', such as theft or fraud,[19] and the unauthorized alteration of computer material, including the intentional damage of software or data; circulation of 'viruses'; and the unauthorised password to a data file; namely; 'crypto viruses'.[20]

This act was criticised severely because of the difficulty of poor monitoring, by the State, in the industry awareness, and the onus to show that the individual committing the unauthorised access was conscious that he or she was not authorised to access such service.[21]

---

15 UK Public General Acts 1990 c. 18 <https://www.legislation.gov.uk/ukpga> accessed 12 February 2021 (Computer Misuse Act 1990).

16 Computer Misuse Act 1990:
'Unauthorised access to computer material —
(1) A person is guilty of an offence if—
(*a*) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured;
(*b*) the access he intends to secure or to enable to be secured, is unauthorised; and
(*c*) he knows at the time when he causes the computer to perform the function that that is the case.
(2) The intent a person has to have to commit an offence under this section need not be directed at—
(*a*) any particular program or data;
(*b*) a program or data of any particular kind; or
(*c*) a program or data held in any particular computer.'

17 Debra Littlejohn Shinder and Michael Cross, 'Building the Cybercrime Case' in DL Shinder and M Cross (eds), *Scene of the Cybercrime* (2nd edn, Syngress 2008) Chapter 14 653-691 <https://www.sciencedirect.com/science/article/pii/B9781597492768000169> accessed 18 August 2020.

18 Mark Osborne, 'Information Security Laws and Regulations', in Mark Osborne (ed), *How to Cheat at Managing Information Security* (Syngress 2006) Chapter 4, 71-86.

19 Osborne, 'Information Security Laws and Regulations', Chapter 4.

20 Osborne, 'Information Security Laws and Regulations', Chapter 4.

21 Osborne, 'Information Security Laws and Regulations', Chapter 4.

Two new laws were passed in 2006 to tackle e-crime. In this regard, the Fraud Act 2006 came into operation in 2007, was intended to eliminate many gaps in anti-fraud laws. The Police and Justice Act 2006 (part 5)[22] amended the CMA.[23] Sections 35 to 38 introduced the increasing of penalties and new offences concerning the misuse in cybercrime. Sections 42 and 43, together with Schedule 13 amended a number of prescriptions in extradition legislation for persons intending to evade the law, as well as the remand and extradition of persons who are serving a sentence in the United Kingdom. Section 44 enables the transfer of prisoners based on international arrangements, but without the consent of such prisoners.[24]

It was recognised practices, guidance and procedures were obsolete and completely insufficient to address electronic evidence in a forensic manner.[25] The initial crime guidelines were published by the Association of Chief Police Officers (ACPO),[26] and referred to as the ACPO Guidelines.

These are acknowledged as the best practice guidelines put together for implementation, enforcement and its approach to digital evidence.[27] This evidence is data expunged from the computer system and must satisfy the five rules regarding evidence, which are: admissibility, authenticity, reliable, and believability.[28] The Tallinn Manuals are also fast becoming the non-binding authoritative manuals applicable to international law insofar as cyber

---

22 Jahankhani and Hosseinian-far, 'Digital forensics education, training and awareness' 91-100.

23 Thomas Wilhelm, 'Ethics and Hacking', in Thomas Wilhelm (ed), *Professional Penetration Testing: Creating and Learning in a Hacking Lab* (2nd edn, Syngress 2013) Chapter 2, 11-36; Abstract: This chapter examines the role that ethics plays in professional penetration testing and identifies different ethical codes of conduct and legal constraints on professional penetration testing; UK Public General Acts 2006 c. 48 <https://www.legislation.gov.uk/ukpga> accessed 18 August 2020.

24 UK Public General Acts 2006 c. 48 <https://www.legislation.gov.uk/ukpga> accessed 18 August 2020.

25 Jahankhani and Hosseinian-far, 'Digital forensics education, training and awareness' 91-100.

26 ACPO (Association of Chief Police Officers), Good Practice Guide for Digital Evidence (July 2007 and subsequently revised in November 2009 and March 2012) <https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evi dence_v5.pdf> accessed 18 August 2020.

27 Jahankhani and Hosseinian-far, 'Digital forensics education, training and awareness' 91-100.

28 Jahankhani and Hosseinian-far, 'Digital forensics education, training and awareness' 91-100.

operations[29] and the relevant legislative frameworks of the two Tallinn Manuals include the laws of; state responsibility, maritime law, international telecommunications, space law, diplomatic and consular law, the general human rights, the general principles of international law, including sovereignty, jurisdiction, due diligence, and the prohibition of intervention.[30]

4.2.2 Investigatory Powers Act of 2016 (IPA)

The IPA determines the degree to which certain of investigatory powers must be utilised for interfering with privacy, and imposes some duties in relation to privacy and its related protections.[31] This Act also gives an updated mechanism for security and intelligence agencies usage, as well as law enforcement and other public authorities, with regard to investigatory powers to acquire communications data.[32] These powers encompass aspects such as communications interception, retaining and acquiring communications data, and interfering with equipment to acquire transmissions and relevant data lawfully, exercising the powers in terms of the Act.[33] It is not lawful to exercise such powers if it relates to the intelligence and security agencies' examination and retention of bulk datasets of a personal nature.[34]

The Act further details the various types of warrants regarding the lawful interceptions of communications. Section 15 addresses the three forms of warrants that could, which are: targeted interception warrants,[35] targeted examination warrants, and mutual assistance warrants. Subsections (2), (3) and (4) provides for the nature of the warrants, in specific terms. Subsection (2) defines a targeted interception warrant relating to the securing of ancillary data.[36] Subsection (3) explains that a 'targeted examination warrant' allows for

---

29 Trishana Ramluckan, 'The Applicability of the Tallinn Manuals to South Africa' 14th International Conference on Cyber Warfare and Security (ICCWS) (2019) 348-355 <https://www.proquest.com/openview/ac4cc9f3edd6ada5ae1cfe838cb65e68/1?pq-origsite=gscholar&cbl=396500> accessed 12 May 2020.

30 Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations General* (2nd edn, Cambridge University Press 2017).

31 Investigatory Powers Act (IPA) 2016 c. 25, s 1, Part 1 - Overview and general privacy.

32 See IPA 2016, Commentary on provisions.

33 IPA 2016.

34 IPA 2016, Commentary on provisions.

35 IPA 2016, Part 2, Chapter 1.

36 IPA 2016, s 15(2).

the inspection of information under a 'bulk interception warrant'.[37] Subsection (3), refers to a targeted examination warrant that authorises the selection of relevant content for inspection, insofar as such examination relates to breach of the prohibition contained in section 152(4).[38] Meanwhile, subsection (4) refers to a mutual assistance warrant, which authorises a person to secure, 'the making of a request in terms of an EU mutual assistance treaty or agreement, or an international mutual assistance agreement', for intercepting communications and disclosing anything acquired under the warrant.[39] Subsection (5) confirms the authorisation of any conduct required to fulfil what is authorisable or demanded by the warrant, including the communications' interception not particularly defined in the warrant itself, or obtaining secondary data from such communications.[40]

This Act also addresses further types of warrants. Section 99 refers to General Warrants under Part 5 and refers to two forms of warrants that could be issued:[41] targeted equipment interference warrants[42] and targeted examination warrants.[43] Section 99, subsection (2), authorises the person securing interference with any equipment for the purpose of acquiring communications, data equipment and any other information. The Act further allocates specific meaning to equipment data as systems data, and a technical description of data.[44] Section 136 deals with bulk interception warrants,[45] where the

---

37 IPA 2016, s 15(3).

38 Prohibition on seeking to identify communications of individuals in the British Islands (IPA 2016). A targeted examination warrant must be sought whenever a member of an intelligence service wishes to look at material which relates to a person who is known to be in the British Islands and when he or she believes that it is necessary and proportionate to select the content of that person's communications for examination.

39 IPA 2016, s 15(4).

40 IPA 2016, s 15(5). For example, a warrant can authorise the interception of communications of other individuals who may use the phone line or email account subject to a warrant. A warrant needs to be able to authorise this conduct because it would not be possible to intercept only those communications belonging to the person that is subject to the interception warrant where other people use the same device.

41 IPA 2016, s 1, Part 5.

42 IPA 2016, sub-s (2).

43 IPA 2016, sub-s (9).

44 IPA 2016, s 100(2).

45 IPA 2016, Part 6, Chapter 1.

interception relates to overseas communications as well as the securing of secondary data from the communications.[46]

Reference to different types of warrants specifying the conduct and details of the warrant will result in fewer infringements on personal rights to privacy as well as protecting personalities.

4.2.3 UK Data Protection Act (DPA)

With regard to the UK-DPA, there are three central pieces of legislation: the General Data Protection Regulation (GDPR), the Data Protection Act 2018[47] (DPA), and the Network and Information Systems Regulations 2018 (NISR). These legislations impose responsibility relating to the protection of personal data.[48] The legal background to the DPA 2018 arose from the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, referred to as Convention 108 which became open for signature in 1981.[49] The Convention is the first internationally binding protecting individuals from possible abuses attendant to collecting and processing of personal data.[50] The Convention contains a regime meant for the governance of that approach, including fair and lawful[51] processing of personal data and storage[52] of data only for specified purposes. Additionally, States must not constrain trans-border flows to other states which signatory part of the Convention.[53] Is noteworthy that the Data Protection Act 1984 was passed and subsequently on the UK ratified the Convention in 1985, which was a mechanism partly to grant free movement of data.[54] The principles immanent to the Data Protection Act 1984 were

---

46 See IPA 2016, s 137.
47 UK Public General Acts 2018 c.12 (Data Protection Act) (hereinafter referred to the DPA 2018).
48 Hayes and Drury, 'Cybersecurity in United Kingdom'.
49 Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Strasbourg, 28 January 1981) <https://www.coe.int/en/web/ conventions/full-list/-/conventions/treaty/108> accessed 8 March 2021 (hereinafter TREATY - ETS No 108).
50 TREATY - ETS No 108, Summary.
51 TREATY - ETS No 108, article 5.
52 TREATY - ETS No 108, article 2.
53 TREATY - ETS No 108, article 12.
54 DPA 2018.

derived almost directly from Convention 108.[55] Therefore, Data Protection Act 1998 is viewed as a repeal of the Data Protection Act 1984.

The UK's Data Protection Act (UK-DPA) 2018,[56] is a supplement of the EU General Data Protection Regulation (GDPR), that came into force on 25 May 2018. Meanwhile, the GDPR was subsequently published in the Official Journal of the European Union.[57] Furthermore, GDPR allocates regulation in respect of collecting, storing, and using personal data in more significant stricter ways.[58] The old Convention 108,[59] was amended to align it with the General Data Protection Regulation,[60] and now referred to as the modernized 'Convention 108+'.[61] According to Secretary General of the Council of Europe, Thorbjørn Jagland, such amendment permits nations to experience and partake in the vigorous precepts that safeguards personal data, providing a special forum for coopetition on an international level.[62] The European Commission also agreed to the contributions of these amendments in relation to relevant approaches regarding high data protection standards.[63] In this regard, the foremost innovations in the modernised Convention 108 include: proportionality,[64] revised focus on data security and additional responsibilities attendant to declaring data breaches,[65] enhanced data processing and transparency,[66] as well as the right of individuals to non-dictatorial practices allowing for person not to be subjected

---

55 DPA 2018, Explanatory note 51.

56 Published on 23 May 2018 - United Kingdom Act of Parliament. Repeals Data Protection Act 1998.

57 Regulation (EU) 2016/679.

58 EU General Data Protection Regulation, <https://www.google.com/search?q=eu+general+data+protection+regulation&rlz=1C1CHBD_enZA770ZA770&oq=EU+General+Data+Protection+Regulation&aqs=chrome.0.0i457j0j46j0l5.1467j0j7&sourceid=chrome&ie=UTF-8> accessed 10 June 2020.

59 TREATY - ETS No 108.

60 Jennifer Baker, 'What does the newly signed "Convention 108+" mean for UK adequacy?' (*The Privacy Advisor*, 30 October 2018) <https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/> accessed 8 March 2021.

61 TREATY - ETS 108+, '128th Session of the Committee of Ministers' (Elsinore, Denmark, 17-18 May 2018) Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf> accessed 8 March 2021.

62 Baker, 'What does the newly signed "Convention 108+" mean for UK adequacy?'.

63 Baker, 'What does the newly signed "Convention 108+" mean for UK adequacy?'.

64 TREATY - ETS 108+, '128th Session of the Committee of Ministers', article 5.

65 TREATY - ETS 108+, '128th Session of the Committee of Ministers', article 7.

66 TREATY - ETS 108+, '128th Session of the Committee of Ministers', article 8 – Transparency of processing.

to a decision solely based on an automatic processing without having their views taken into consideration.[67] Article 9(2) allows exemption of data controllers from exercising some of these requirements for specified purposes, such as protection of national security.[68]

The DPA, together with the GDPR, refers to the personal data processing.[69] Article 1 of the GDPR premises on protecting individuals' data protection rights. Chapter 2 of Part 2[70] relates to the GDPR and extends to the processing of personal data within the United Kingdom jurisdiction. The GDPR also locate supplementary overview of the Act and its particular focus on the protection of the rights of individuals; regarding the processing of personal data.[71] The definition of personal data is defined as:

> Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[72]

This provision was used against Google and set a historic precedent. In this regard Google was fined 50 million euros,[73] or about $57 million by the French data protection authority, for improper disclosure to users about its collection of data because this penalty is the largest since the European Union General Data Protection Regulation came into force,[74] which is emblematic of the view that regulators do follow up on the rules to find things on the Internet companies

---

67 TREATY - ETS 108+, '128th Session of the Committee of Ministers', article 9 – Rights of the data subject.

68 TREATY - ETS 108+, '128th Session of the Committee of Ministers', article 9(2) – para 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

69 DPA 2018, s 2 – Protection of personal data.

70 DPA 2018.

71 DPA 2018, para 8 – Commentary on provisions.

72 DPA 2018, s 3 – Terms relating to processing of personal data.

73 EDPB (European Data Protection Board), 'The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC' (21 January 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> accessed 31 May 2020.

74 Adam Satariano, 'What the G.D.P.R., Europe's Tough New Data Law, Means for You' *The New York Times* (New York, 6 May 2018) <https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html> accessed 25 May 2020.

whose core businesses rely on collecting data.[75] Facebook is also being investigated by several data protection authorities in Europe.[76] It is noted that the penal measure imposed on Google is reportedly the fourth largest penalty to date.[77]

4.2.4 Network and Information Systems Regulations of 2018 (NISR)

The purpose of the NISR[78] is to ensure that essential services such as health, energy, water, transport, and digital infrastructure together with certain service providers have set up efficient procedures for improving security. The Act further focuses on the limitation of the disruption of services to prevent serious harm[79] to the economy, individuals' welfare along with society at large. The Act ensures that severe occurrences be disclosed expeditiously to the relevant officials.[80] These Regulations arise from the enforcement of the directive on 'Security of Network and Information Systems (EU) 2016/1148)', where members had up to May 2018 to incorporate the Directive into the domestic law. The aim of such incorporation is to make sure that the UK is resilient, secure from virtual threats, affluent and self-assured in a robotic society,[81] whilst, the 'National Cyber-Security Centre' (NCSC) responds to internet safety incidents.[82]

The Government took a collective proficient authority approach, instead of founding a sole governmental body, in order to make sure that all officials need to be competent have a comprehension of their sectors as well as encouraging the mainstreaming of cybersecurity,[83] the NCSC a single point of contact[84] and a Computer Security Incident Response Team.[85]

---

75 Satariano, 'What the G.D.P.R., Europe's Tough New Data Law, Means for You'.
76 Satariano, 'What the G.D.P.R., Europe's Tough New Data Law, Means for You'.
77 EDPB, 'Baden-Württemberg supervisory authority issues first German GDPR fine' (22 November 2018) <https://edpb.europa.eu/news/national-news/2018_en> accessed 6 June 2020.
78 UK Statutory Instruments 2018 No 506 (Network and Information Systems Regulations 2018) (NISR) <https://www.legislation.gov.uk/uksi> accessed 8 March 2021.
79 Events such as the 2017 WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 attack on Ukraine's electricity network clearly highlight the impact that can result from adversely affected network and information systems.
80 NISR 506, para *2.*
81 NISR 506 Explanatory Memorandum, para 4.
82 NISR 506, Part 2, s 2.
83 NISR 506, Part 2, s 3.
84 NISR 506, Part 2, s 4.
85 NISR 506, Part 2, s 5.

The NCSC undertakes its duties in respect of the regulations when acting in the execution of its functions as directed by the Intelligence Services Act.[86]

4.2.5 Fraud Act of 2006 (FA)[87]

The above mentioned Act provides a three-fold context of commission of general offence: by false pretext representation,[88] failure to disclose information[89] and by using position for abuse.[90] In addition, the Act creates a regime of new offences by means of which services are obtained dishonestly,[91] possessing, making and supplying articles for fraudulent use.[92] Therefore, it is a punishable transgression to make, adapt, supply or provide an article knowing that it is intending to use such article to directly commit or facilitate the action of fraud.[93] For example, an individual manufactures and produces devices which, when attached to electricity meters, cause the meter to dysfunctional. Section 8 expands the meaning of 'article' as encompassing any data or program held electronically. Examples of the fraudulent use of electronic programs or data include, but not limited: a computer programme used for generating credit card numbers; using computer templates to produce blank utility bills; using computer files to obtain credit card details or draft letters belonging to other people the process of obtaining 'advance fee' funds.[94] South Africa still relies on the common law for fraud offences.

---

86 Intelligence Services Act 1994, s 3(1)(*b*). UK Public General Acts 1994 c. 13 <https://www.legislation.gov.uk/ukpga> accessed 8 March 2021.
'(*b*) to provide advice and assistance about—
(i) languages, including terminology used for technical matters, and
(ii) cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or, in such cases as it considers appropriate, to other organisations or persons, or to the general public, in the United Kingdom or elsewhere.'

87 UK Public General Acts 2006 c. 35 <https://www.legislation.gov.uk/ukpga> accessed 9 March 2020 (Fraud Act) (hereinafter FA 2006).

88 FA 2006, s 2.

89 FA 2006, s 3.

90 FA 2006, s 4.

91 FA 2006, s 11.

92 FA 2006, s 6.

93 FA 2006, s 7 – Making or supplying articles for use in frauds of the FA.

94 FA 2006, s 8 para 28, Commentary on Act <https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5> accessed 9 February 2021.

4.3 European arrest warrant (EAW)

The Framework Decision[95] takes the 'approach by abolishing extradition and by replacing it with a system of surrender between judicial authorities, based on mutual recognition and on the free movement of judicial decisions, which results from a high level of confidence between the Member States'.[96] The Court made rulings pertaining to: the validity of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European warrant of arrest; the procedures for surrender between Member States, the abolishment of the double criminality requirement for offences listed Article 2(2) of the Framework Decision, and found that such requirement did not constitute the contravention of the principle of legality in criminal proceedings, or the equality principle as contained in Article 6(2) Treaty of the EU.[97]

The EAW states that formal procedures for extradition ought to be abolished among the Member States with regard to persons fleeing justice after sentencing and extradition procedures, and such procedures to be expedited in the context of persons suspected of having committed an offence.[98] Paragraph 8, of the EAW alludes that execution decisions of the European warrant of arrest should be subjected to adequate judicial authority and controls. Paragraph 9 refers to the responsibilities of the central authorities in the executing of an EAW which should be curtailed to the extent of participative assistance. Paragraph 13, on the other hand, stated that no individual shall be extradited to a State where the death penalty, torture or other inhumane treatment were practised.

---

95 Council of the European Union, 'Council Framework Decision'.

96 Case law – Belgium - Opinion of Mr Advocate General Ruiz-Jarabo Colomer delivered on 12 September 2006. *Advocaten voor de Wereld VZW v Leden van de Ministerraad* Case C-303/05. Reference for a preliminary ruling: Arbitragehof - Belgium. Police and judicial cooperation in criminal matters - Articles 6(2) EU and 34(2)(*b*) EU - Framework Decision 2002/584/JHA - European arrest warrant and surrender procedures between Member States - Approximation of national laws - Removal of verification of double criminality - Validity. Case C-303/05. *European Court Reports* 2007 I-03633 ECLI identifier: ECLI:EU:C:2006:552 para 46 of Judgement <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62005CC0303> accessed 12 February 2021.

97 *Advocaten voor de Wereld VZW v Leden van de Ministerraad* Case C-303/05 para 108.

98 Paragraph 1 of the C: 2006:552; Council of the European Union, 'Council Framework Decision'.

Article 2(2), of the EAW is an important central tenet of double criminality, but is not applicable to 32 listed offences,[99] and is subject to the proviso of associate States issuing such extradition, imposes penalties for these infractions with a sentence not exceeding least three years.

Article 3 refers to three instances for mandatory non-execution of the European arrest warrant, while Article 4 establishes several grounds for optional non-execution, including where the convicted person is a national or resident.[100] Unlike the traditional extraditions, the EAW's proceedings are addressed urgently within time-bound specificity.[101] The EAW must contain the information necessary and the annexure is attached for the purposes of consistency.[102] Provision is also made for difficulties arising from the procedure which should be addressed by the courts.[103] The EAW further makes provision for transgression apart from those addressed in Paragraph 2.[104] Article 6 refers to determinations to be made by the competent judicial authorities,[105] while judicial oversight is mandatory. However, the EU and the UK agreed on the terms of

---

99 Participation in a criminal organisation, for example:
- terrorism,
- trafficking in human beings,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,
- fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995,

100 Article 4(6) 'if the European arrest warrant has been issued for the purposes of execution of a custodial sentence or detention order, where the requested person is staying in, or is a national or a resident of the executing Member State and that State undertakes to execute the sentence or detention order in accordance with its domestic law' Article 5(3) 3. 'Where a person who is the subject of a European arrest warrant for the purposes of prosecution is a national or resident of the executing Member State, surrender may be subject to the condition that the person, after being heard, is returned to the executing Member State in order to serve there the custodial sentence or detention order passed against him in the issuing Member State'.

101 Articles 17 and 23.

102 Article 8.

103 Article 10(5).

104 Article 2(4) 'For offences other than those covered by paragraph 2, surrender may be subject to the condition that the acts for which the European arrest warrant has been issued constitute an offence under the law of the executing Member State, whatever the constituent elements or however it is described.'

105 Article 6(2) 'the executing judicial authority shall be the judicial authority of the executing Member State which is competent to execute the European arrest warrant by virtue of the law of that State'.

the UK leaving the EU[106] through the Trade and Cooperation Agreement.[107] Following such departure from the EU (Brexit) at 11pm on 31 December 2020 as such, the European Arrest Warrant ceased from applying to the UK, but applies to persons who are arrested for valid reasons under a European Arrest Warrant prior to Brexit moment.[108] Acting against the warnings of senior law enforcement officials, the UK abandoned a crucial tool that sped up the transfer of criminals across borders with other European states.[109] One of the biggest practical losses is access to information sharing system amongst all EU 27 and some states provided for real-time information sharing from police databases.[110] However, the UK is not a member anymore of Europol, Eurojust and the Schengen Information System II[111] as such, its requests will not be prioritised.[112] The EU-UK Trade and Cooperation Agreement to its credit,

---

106 British Exit, 'The withdrawal of the United Kingdom from the European Union' (2021) <https://www.google.com/search?q=brexit+meaning&rlz=1C1GCEU_enZA821ZA822&oq=br&aqs=chrome.0.69i59j69i57j69i59j0i67l2j69i60l3.2671j0j7&sourceid=chrome&ie=UTF-8> accessed 15 July 2021.

107 EUR-Lex 'Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part' L 444/14 - Official Journal of the European Union 31.12.2020: part three: Law Enforcement and Judicial Cooperation in Criminal Matters 300 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.444.01.0014.01.ENG> accessed 15 July 2021.

108 *Marek Polakowski, Vijay Sankar, Carlos Mendes, Maris Zelenko and Thomas Ovsianikovas Applicants v (1) Westminster Magistrates' Court and 6*, Neutral Citation Number: [2021] EWHC Civ 53 (Admin) para 32 on 5 <https://vlex.co.uk/vid/marek-polakowski-vijay-sankar-855846856> accessed 15 July 2021; Louisa Collins, 'European Extradition after Brexit: What now?' (25 January 2021) <https://www.5sah.co.uk/knowledge-hub/news/2021-01-27/high-court-clarifies-status-of-ongoing-eaws-post-brexit> accessed 15 July 2021; BAILII 'England and Wales High Court (Administration Court) Decisions' (20 January 2021) <https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Admin/2021/53.html& query=(josse)+AND+(extradition)> accessed 15 July 2021.

109 Jamie Grierson, Jennifer Rankin and Lisa O'Carroll 'UK to withdraw from European arrest warrant' *The Guardian* (United Kingdom, 27 February 2020) <https://www.theguardian.com/uk-news/2020/feb/27/uk-to-withdraw-from-european-arrest-warrant> accessed 15 July 2021.

110 Áine Kervick, 'Extradition post-Brexit: the TCA at a glance' (29 January 2021) <https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/extradition-post-brexit-the-tca-at-a-glance> accessed 15 July 2021.

111 *Marek Polakowski, Vijay Sankar, Carlos Mendes, Maris Zelenko and Thomas Ovsianikovas Applicants v (1) Westminster Magistrates' Court and 6*, Neutral Citation Number: [2021] EWHC Civ 53 (Admin) para 32 on 5 <https://vlex.co.uk/vid/marek-polakowski-vijay-sankar-855846856> accessed 15 July 2021.

112 Kervick, 'Extradition post-Brexit: the TCA at a glance'.

contains similar extradition rules and procedures to the European Arrest Warrant protocols.[113]

The UK has comprehensive cybersecurity laws, that are statute-based.[114] According to which fraud is addressed primarily by means of the Computer Misuse Act 1990 (CMA). Similarly, the United States also has a Computer Fraud and Abuse Act to address computer offences. The next section addresses the United States context of Computer Fraud and related offences to some extent. Amongst all 27 EU Member States it's providing for real-time, real time when with information sharing from police databases. However, UK is not a member anymore of Europol, Eurojust in the Schengen Information System II as such; its request will not be prioritised. The EU-UK Trade and cooperation agreement has similar rules and procedures.

4.4 United States context

4.4.1 Computer Fraud and Abuse Act (CFAA)[115]

The CFAA of 1984, only introduced three new Federally declared crimes to cover certain conduct by a person who 'knowingly accesses a computer without authorisation, or accessed a computer with authorisation and uses the opportunity for purposes to which such authorisation does not extend'.[116] The crimes relating to government's interests were indicated as: the misuse of computers to obtain national security secrets, computer misuse to obtain financial records of a personal nature, and hacking into government computers belonging to the government.[117] The CFAA was enacted in 1986, as an amendment to the first federal computer fraud law,[118] and Congress

---

113 Citizens Information, 'Extradition to and from Ireland' (13 January 2021) <https://www.citizensinformation.ie/en/justice/arrests/extradition_to_and_from_ireland.html#l414a7> accessed 15 July 2021.

114 Hayes and Drury, 'Cybersecurity in United Kingdom'.

115 Computer Fraud and Abuse Act 1984, Coded as 18 U.S.C. § 1030, which is changed into the Computer Fraud and Abuse Act in 1986.

116 18 U.S.C. § 1030(*a*)(1)-(2).

117 18 U.S.C. § 1030(3).

118 NACDL, 'CFAA Background'. In 1984, Congress passed the Comprehensive Crime Control Act, which included the first federal computer crime statute.

significantly expanded the computer crime statute by passing the CFAA.[119] It was the intention of congress to prevent the unauthorised access to 'federal interest' computers and to amend additional penalties pertinent to fraud and related activities connected to accessing devices and computers, as well as providing protection to such computers of interest.[120] In this regard, The CFAA[121] added three new prohibitions: 'Section 1030(*a*)(4) prohibiting unauthorized access with intent to defraud; section 1030(*a*)(5) prohibiting accessing a computer without authorization and altering, damaging, or destroying information; and section 1030(*a*)(6) prohibiting trafficking in computer passwords'.

The statute, was initially intended to criminalise only important (federal interest) computer crimes,[122] but potentially regulates every use of every computer in the United States and even many millions of computers abroad.[123] Congress further added private civil liability for CFAA transgressions for injury suffered and receiving reparations or other fair remedy.[124] The Act was broadened covering various cyber acts, extending to: larceny as a component of a plan for the purpose of embezzlement;[125] variation,[126] destruction, distribution of malevolent codes and denial of service and password peddling.[127] Section 1030(*a*)(5) was amended for the purpose of further protecting networks from harm or destruction that was unintended. The section was expanded to include both, outsiders acquiring unofficial access, and to insiders who intentionally cause destruction to a computer.[128] The scope of conduct was broadened to also include transmissions.[129] With such revision, the trajectory of the Act moved

---

119 NACDL, 'CFAA Background'. The CFAA was the 1986 amendment to 18 U.S.C. § 1030; however, 18 USC § 1030 in its entirety is commonly referred to as the Computer Fraud and Abuse Act and *vice versa*.

120 NACDL, 'CFAA Background'.

121 18 USC § 1030.

122 Part 1.

123 Orin S Kerr, 'Vagueness challenges to the Computer Fraud and Abuse Act' (2010) 94 Minnesota Law Review 1561.

124 18 USC § 1030(*g*).

125 18 USC § 1030(*a*)(4).

126 18 USC § 1030(*e*)(6).

127 18 USC § 1030(*a*)(6).

128 NACDL, 'CFAA Background'.

129 Section 1030(*a*)(5)(A) specifically prohibiting 'knowingly caus[ing] the transmission of a program, information, code, or command' which 'intentionally causes damage without authorization'.

from a technicality concept of access to the suspects aim to inflict harm.[130] Congress constantly expanded the CFAA with later revisions in '1996, 2001, 2002, and 2008'.[131]

4.4.2 Economic Espionage Act (National Information and Infrastructure Protection Act of 1996 (NIIPA)[132]

In 1996, Title II of the Economic Espionage Act[133] dramatically expanded the statute in three different forms.[134] Firstly, the coverage of 'section 1030(*a*)(2)'[135] extended the prohibition to prohibited access for any intelligence of any type where the actions related to foreign or interstate transmissions. Secondly, new provisions were added to the computer damage prohibition in '§ 1030(*a*)(2)',[136] and a 'computer extortion' act at '§ 1030(*a*)(7)'.[137] The NACDL argued that at §°'1030(*a*)(2)' converted a misdemeanour into an offence a computer extortion statute at §°1030(*a*)(7).[138] The NACDL argued that a felony enhancement at

---

130 NACDL, 'CFAA Background'.

131 NACDL, 'CFAA Background'.

132 § 290001(*d*), 108 Stat at 2098.

133 EEA 18 USC § 1834.

134 NACDL, 'CFAA Background'.

135 Originally limited to unauthorized access that obtains financial records from financial institutions, card issuers, or consumer reporting agencies.

136 Section (*a*)(2) 'intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in Section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer'.

137 Section (*a*)(7) 'with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any-
(A) threat to cause damage to a protected computer;
(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.'

138 Section (*a*)(7) 'with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any-
(A) threat to cause damage to a protected computer;
(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.'

§°1030(*a*)(2) converted a misdemeanour violation into a felony.[139] The third significant change was replacing the category of 'federal interest' computers with the new category of 'protected computers'.[140] In this regard, the NACDL alluded the flaw in the Act regarding the clarity of whether the word 'use' in trade and business also applied to use in the realm criminal wrongdoing or generally, because of the anomaly of every computer used in interstate commerce would be a 'code protected computer' under section 18 ('U.S.C. § 1030'). It was argued that this could constitute some form of over criminalisation.[141]

4.4.2.1 National Information and Infrastructure Protection Act of 1996 (NIIPA)

The NIIPA 1996 broadened the terrain of the original statute. Firstly, subsection (*a*)(2) is expanded,[142] to information of any sort that is stored on any computer, that is protected, only on account of a foreign or interstate element being in this conduct.[143] Secondly, a new form of offence was included to penalise computer extortion.[144] Thirdly, by expanding the list of damage,[145] it increased the range of computer damage and two new forms of damages were added, including 'physical injury to any person'[146] and 'a threat to public health or safety'.[147]

---

139 If the offense was conducted in furtherance of any crime or tortious act, if it was conducted for purposes of financial gain, or if the value of the information obtained exceeded $5,000.

140 The latter category now merely required a machine 'used' in interstate commerce; as opposed to the former, which required computers used in two or more states.

141 National Association of Criminal Defence Lawyers (NACDL) 'Computer Fraud and Abuse Act (CFAA)' <https://www.nacdl.org/Landing/ComputerFraudandAbuseAct> accessed 15 May 2021.

142 Initially, only the computers used by financial institutions, card issuers, or consumer-reporting agencies were protected.

143 18 U.S.C. § 1030(*a*)(2)(C) (1996) Initially, only obtaining information contained on a financial record of a financial institution or in a file of a consumer reporting agency on a consumer was criminalised;466 and after 1996 any obtaining of information shall be punished, as long as the computers involved locate in more than one states.

144 18 U.S.C. § 1030(*a*)(7).

145 Prescribed in § 1030(*c*)(4)(A)(i).

146 18 U.S.C. § 1030(*c*)(4)(A)(i)(III) (1996).

147 18 U.S.C. § 1030(*c*)(4)(A)(i)(IV) (1996).

4.4.3 USA Patriot Act[148] *and the Freedom Act (H.R. 2048)*

Due to the attack on the World Trade Centre in 2001, this prompted the passing of the succeeding generation of the CFAA by way of the 'USA Patriot Act'. In this regard, of utmost prominence was the broadened scope of the definition of 'protected computer' and encompassing computers beyond the borders of the US used in ways which affects trade or economics in America.[149] This Act triggered further crimes in terms of '§ 1030(*a*)(5)' by augmenting damage or harm of 'any computer used'.[150] The USA Freedom Act (H.R. 2048) was promulgated as law on 2 June 2015, which re-established and revised various sections in the Patriot Act, which curtailed the government's authority to collect data.[151] In this regard, the USA Freedom Act of 2015 banned the collection of bulk private records of Americans which was stipulated in section 215 of the USA Patriot Act.[152]

4.4.4 Prosecutions of offences: The case of United States of America versus Vladimir Tsastsin and 6 others

The indictment[153] in the matter of *United States of America Versus Vladimir Tsastsin and 6 others*, deals with the prosecution of cyber offences. The said offences in this case related to wire fraud.[154]

---

148 Title III of the USA Patriot Act of 2001, also known as 'The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001' (the Act) is intended to make it more difficult for terrorists to launder money in the United States <https://www.govinfo.gov/con tent/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf> accessed 2 July 2021.

149 Section 814(*d*) the USA Patriot Act of 2001.

150 Section 814(4)(*B*)(v) the USA Patriot Act of 2001.

151 Legal Sidebar, 'USA Freedom Act Reinstates Expired USA Patriot Act Provisions but Limits Bulk Collection' (6 April 2015) <https://fas.org/sgp/crs/intel/usaf-rein.pdf> accessed 2 July 2021.

152 The USA Freedom Act <https://www.leahy.senate.gov/imo/media/doc/USA%20FREEDOM%20One-Pager%20-final.pdf> accessed 2 July 2021.

153 United States District Court, Southern District of New York, Sealed Indictment 82-11 Cr-878 United States of America Versus Vladimir Tsastsin, Andrey Taamei, Timur Gbrassimenko, Dmitri Jegorov, Valerri Aleksejev, Konstantin Poltev and Anton Ivanov. The *United States Attorney's Office 'United States v Vladimir Tsastsin* Et Al 11 CR 878' (9 November 2011) <https://www.justice.gov/usao-sdny/programs/victim-witness-services/united-states-v-vladimir-tsastsin-et-al-11-cr-878> accessed 15 May 2021.

154 18 U.S.C. § 1343 - The Wire fraud statute, which requires proof of many elements similar to those needed for s 1030(*a*)(4) but carries stiffer penalties.
Title 18, United State Code, s 1030(*a*)(4) provides:
'Whoever—

The indictment provides an overview of the modus operandi of the defendants and their co-conspirators. These are offences of (i) 'click hijacking fraud' and (ii) 'advertising replacement fraud'.

The intricate and massive fraud scheme through their own publisher networks and using malware to fraudulently divert Internet traffic to certain advertiser websites,[155] is explained in detail; with the exhibits of the scheme; with the manipulation of the Domain Name System (DNS) servers and with malware designed to modify or alter the DNS.[156]

4.5 Conclusion

Section 1 of the UK CMA,[157] articulates that causing a computer to authorise illegal access while operating on the Internet is a punishable transgression. Section 2 articulates intention, and that unauthorised access for commissioning further transgressions and unauthorised activities for impairing computers constitutes criminal offences.[158] The CMA was supplemented with further acts, as the UK recognised the difficulty of obtaining digital evidence rather than 'hard evidence' which is difficult in securing, in respect of defining the character of the evidence, and categorising as a digital evidence with credibility in court.[159]

The UK Investigatory Powers Act 2016 (IPA) is a critical piece of legislation which helps to facilitate the creation of improvement of South African

---

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . . shall be punished as provided in subsection (*c*) of this section.'

155 Indictment para 19 at 13.

156 Indictment para 20 at 14. At para 21 – a computer user can access a website on the Internet by either two ways: by entering into the computer's web browser either the Internet Protocol address or the domain name for that website. The IP address is a unique numerical address associated with a website (e.g., 123.45.6.78), akin to a home or business street address, whereas a domain name is a simple, easy to remember way for humans to identify computer on the Internet (e.g., www.Irs.gov).

157 Computer Misuse Act 1990.

158 Sharma, 'Legislation Related to Cyber-Crimes in United Kingdom'.

159 Jahankhani and Hosseinian-far, 'Digital forensics education, training and awareness' 91-100.

cybersecurity law. The IPA provides uniform statutory safeguards and articulates the powers of different public authorities how they can be used and for what purposes. The statutory tests are prescribed and should be complied with prior to the usage of any power. Such test includes the authorisation regime for each investigative instrument, including for Judicial Commissioners to approve the issuance of warrants; as well as a new requirement pertaining to highly delicate and invasive laws.[160] The Act further brings about provision for overseeing the implementation, and gives authority to the 'Secretary of State' in respect of records from service providers.[161]

The UK DPA augments, adds and allows for exceptions in the legal framework of the UK 'GDPR'. It in addition directs the process of information by different offices; the 'Serious Fraud Office, the Financial Conduct Authority (FCA) and the National Crime Agency (NCA)'.[162] This Act is concerned with the processing of personal data, subject to the GDPR. Meanwhile, The DPA complements the GDPR[163] while Chapter 3, institutes a broad mechanism certain forms of processing to which the GDPR does not subscribe.[164] The processing of data must be by competent authorities,[165] includes the intelligence services.[166] The Act also makes provision about the Information Commissioner[167] and enforcement of the data protection legislation.[168]

The EAW is considered the most prominent piece of legislation in extradition's history, especially insofar as simplifying those procedures.[169] While it prohibits the traditional obstacles in instances of political drama, military, fiscal offenses and non-transmission by citizens; extradition proceedings are waived in two stages.[170] The phrase 'extradition' is replaced with the phrase 'surrender', and the terms 'applicant State' and 'soliciting' state are replaced with 'issuing judicial authority and enforcement' or 'the issuing State and the executing Member

160 IPA 2016, ss 227-240 Part 8 – Oversight arrangements.
161 IPA 2016, s 87 Part 4 – Retention of communications data.
162 Hayes and Drury, 'Cybersecurity in United Kingdom'.
163 DPA 2018, Part 2, Chapter 2 – General processing.
164 DPA 2018, Part 2, Chapter 3.
165 DPA 2018, Part 3 deals with 'Law enforcement processing'.
166 DPA 2018, Part 4 deals with 'Intelligence services processing'.
167 DPA 2018, Part 5 deals with 'The Information Commissioner'.
168 DPA 2018, Part 6 deals with 'Enforcement'.
169 Pinteală, 'Legal aspects of the European arrest warrant'.
170 Pinteală, 'Legal aspects of the European arrest warrant'.

State'.[171] In this regard, Member States may still apply or to sign bilateral or multilateral agreements to facilitate and simplify the procedures.[172] However, UK's departure from the EU regime is now governed by the Trade and Cooperation Agreement[173] and referred to as the Arrest Warrant, similar to the European Arrest Warrant extradition's rules and procedures.[174]

The rapid rate in computer technology developments, combined with extant broadening by revision, makes the US 'CFAA' too wide and extensive in the laws of crime, punishment and criminal liability.[175] Congress's willingness to expand criminal liability in areas of developing technology demonstrates a spiralling trend of expansion. Kerr, argues that the remarkable scope of the CFAA requires courts should adopt narrower interpretations in consideration of void-for-vagueness doctrine.[176] Violations of the CFAA generally require access that is unauthorised, either an 'access without authorization' or an act that 'exceeds authorized access'.[177] Remarkably, the meaning of 'unauthorized access' is opaque,[178] and the CFAA is rather too broad for application without careful attention to the vagueness doctrine.[179]

The CFAA, and the US Indictment[180] regulates offenses relating to: hijacking, advertising replacement fraud,[181] conspiracy to commit computer intrusion,[182] wire fraud charge, computer intrusion furthering fraud and computer intrusion by Transmitting data. South Africa's Cybercrimes Act[183] creates new cybercrime

---

171 Council of the European Union, 'Council Framework Decision'.
172 Pinteală, 'Legal aspects of the European arrest warrant'.
173 Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community.
174 Citizens Information, 'Extradition to and from Ireland'.
175 NACDL, Computer Fraud and Abuse Act (CFAA).
176 Kerr, 'Vagueness challenges to the Computer Fraud and Abuse Act' 1561.
177 18 USC § 1030 (*a*).
178 Kerr, 'Vagueness challenges to the Computer Fraud and Abuse Act' 1562, refers to in *United States v Drew* 259 F.R.D. 449 (C.D. Cal. 2009), the government argued that violations of Terms of Service (TOS) render access to a computer unauthorized. In *United States v Nosal*, No CR 08-00237 MHP, 2009 WL 981336 (N.D. Cal. Apr. 13, 2009), the government argued that an employee who accesses an employer's computer with illicit motives to hurt the employer accesses that computer without authorization.
179 Kerr, 'Vagueness challenges to the Computer Fraud and Abuse Act' 1563.
180 United States District Court.
181 Indictment para 4 at 5-6.
182 18 USC § 1030 sections 1030(*a*)(4), (*a*)(5)(A) and (B), (*c*)(3)(A) and (*c*)(4)(A) and (B).
183 Cybercrimes and Security Bill, Republic of South Africa Republic of South Africa, vol 416 (2017).

offences.[184] However, can these new offences compare to the US-CFAA, especially in respect of an extradition request? It may be argued that the Cybercrimes Bill broadly covers the double criminality in respect of the US CFAA and Wire Fraud Statute, However, it is hugely problematic on the issue of specialty, which means that the individual being extradited will only be tried for offences listed in the request, which is a rule in international customary law and which forms part of South African law.[185] Its absence, therefore, would therefore, be in violation of South African law.[186]

A comparative study with worldwide trends and systems in policing, including the APCO guidelines, was undertaken to determine whether or not policing in South African's systems, policies, models, frameworks, and models were sufficient and workable.[187] One of the recommendations of the study was that there is a need for a global approach to policing.[188]

In this chapter various laws affecting extradition were discussed. A further question which now comes to mind is if there are other instruments, like Mutual Legal Assistance, which could aid in extradition proceedings. This will be discussed next, but first an overview of the rule of law will be given to provide perspective for that discussion. This forms part of questions in the next chapter, which first presents an overview of the role to contextualise that discussion.

---

184 Cybercrimes Act 19 of 2020.

185 Neville Botha, 'Lessons from Harksen: a closer look at the constitutionality of extradition in South African law' (2000) 33 CILSA 274, 286.

186 Botha, 'Lessons from Harksen' 286.

187 Vusi E Sithole, 'Policing Frameworks, Policing Systems, Policing Strategies, and Policing Models within the South African Context' (7-9 February 2017) <https://www.saps.gov.za/resource_centre/publications/dr_sithole_policing_frameworks_systems_and_stratetgies.pdf> accessed 12 May 2020.

188 Sithole, 'Policing Frameworks, Policing Systems, Policing Strategies, and Policing Models within the South African Context'.

Chapter 5: Rule of law, *aut dedere aut* judicare (extradite or trial), and mutual legal assistance

5.1 Introduction

The core principle in the rule of law entails that people and the powers that be in particular country, become bound by both current and future laws in an open free society with judicial oversight.[1] South Africa endorsed an implemented Rome Statute bypassing the domestic legislation requirements with the Implementation of the Rome Statute of the International Criminal Court Act.[2] The anomaly arises insofar as failing to abide by the rule of law in cases involving high-ranking individuals.[3] In spite of the implementation and adoption of the Rome statute, there appears to be selective implementation[4] which is inconsistent with the Constitution.[5]

Where there is no treaty, there could be no obligation to extradite, but the State could be obliged to surrender the offender or to punish such offender under its own laws.[6] The nationality exception shifted a lot of attention to the *aut dedere aut* judicare principle because the use of the *aut dedere aut* judicare principle is for either extraditing the perpetrator or establishing due jurisdiction.[7] There are exceptions that prevent extraditions, namely; the political offence exception; the

---

1 Bingham, *The rule of law* 9: 'The idea of the rule of law as the foundation of modern statutes and civilisations have recently become more talismanic than that of democracy.'

2 Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002, Vol 445.

3 Ramjathan-Keogh, 'South Africa, Apartheid, Crimes against humanity and the Rule of Law'.
'South Africa's refusal in 2015 to arrest former Sudanese President Omar al-Bashir whilst h attending the African Union Summit in Johannesburg is a stark reminder of the country's willingness to facilitate impunity and disrespect for the rule of law. Al Bashir is wanted by the International Criminal Court relating to crimes against humanity, war crimes and genocide. The case of the former head of Rwandan intelligence, Kayumba Nyamwasa, from June 2010 is also another situation where South Africa shielded a person implicated in the commission of egregious crimes who is the subject of various extradition requests by granting him refugee status. Nyamwasa continues to reside in South Africa.'

4 *UN Report March 2016.* United Nations Committee noted the failure to detain Omar al-Bashir, President of Sudan in June 2015, pursuant to an International Criminal Court arrest warrant.

5 *UN Report March 2016*. Concern that President Al-Bashir was authorized to leave the country in violation of an interim court order.

6 Watney, 'A South African perspective on mutual legal assistance' 298.

7 Watney, 'A South African perspective on mutual legal assistance' 298.

military offence exception; the fiscal offence exception,[8] although the violations of a State's revenue laws from extradition is under pressure; the death penalty exception,[9] unless reassurance is given of the non-implementation of the death penalty; and the principle of non-discrimination which outlaws extradition[10] where an accused could face prosecution or prejudice on the grounds of race, religion, nationality or political opinions.[11] Article 6 of the Convention[12] addresses the extradition of nationals, and the right to refuse extradition of said nationals. If the party being requested does not extradite its national, then the case must be submitted to the competent authorities.[13] The reason for retaining the nationality exception appears to be the fear, shared by many States, that foreign tribunals will not afford their nationals a fair trial or appropriate punishment.[14]

Mutual Legal Assistance is imperative for extraditions and investigations. The European Convention on Mutual Assistance recognises that extradition is jointly linked to mutual legal assistance, and already acknowledged at the time of signature of the Convention in '1957'.[15] Expeditiousness is important.[16]

---

8 *GG* 24872 of 13 May 2003 Vol 455 (European Convention on Extradition (and the Two Additional Protocols)) art 5.

9 *GG* 24872, art 11.

10 Boister, 'The trend to "universal extradition"' 301.

11 UN General Assembly 'Convention Relating to the Status of Refugees' (28 July 1951) Vol 189, article 3 (available at <https://treaties.un.org/Pages/ViewDetailsII.aspx?src=TREATY&mtdsg_no=V-2&chapter=5&Temp=mtdsg2&clang=_en> accessed 30 April 2021.

12 *GG* 24872.

13 *GG* 24872, art 6(2) 'If the requested Party does not extradite its national, it shall at the request of the requesting Party submit the case to its competent authorities in order that proceedings may be taken if they are considered appropriate. For this purpose, the files, information and exhibits relating to the offence shall be transmitted without charge by the means provided for in article 12, paragraph 1. The requesting Party shall be informed of the result of its request.'

14 Boister, 'The trend to "universal extradition"' 299.

15 European Convention on Mutual Assistance in Criminal Matters 'European Treaty Series – No 30' <https://rm.coe.int/16800656ce> accessed 14 January 2021.

16 T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime (2-3 December 2014) <https://rm.coe.int/16802e726c> accessed 12 May 2020 (hereinafter referred to as T-CY Assessment Report). Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction Adopted by the 12th Plenary of the T-CY (2-3 December 2014). The report has been prepared by the Transborder Group of the Cybercrime Convention Committee (T-CY) in response to a decision taken by the 10th Plenary of the T-CY (2-3 December 2013). For full report see <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf> accessed 12 May 2020.

5.2 Rule of law

5.2.1 Rule of law and its application if no offence exists at the date of the request of the extradition

The expression that was born since the time of Aristotle is that 'no man is above the law'.[17] The principle of legality[18] and the maxims *nullum crimen sine lege* (no crime without a law) and *nulla poena sine lege* (no punishment without a law), is trite law, and this ancient rule of law is the foundation of modern statutes and civilisations.[19] The effect of this is that an extradition would be unlawful if the correct procedures were not followed.[20] The case of Kayumba Nyamwasa former head of Rwanda's Intelligence Services, is yet another example of disregard for the rule of law. South Africa granted him refugee status whereas had been implicated in egregious transgressions and has been the subject of several extradition requests by his own country.[21] Another example pertains to Guus Kouwenhoven, a Dutch war criminal who was convicted for his complicity in war crimes during the presidency of Charles Taylor in Liberia. In this regard, the Netherlands made a request for his extradition in December 2017, so that he serves his 19-year sentence in that country. Surprisingly, South Africa issued him with visa and he continues to live unperturbed in Cape Town.[22] However, the State's appeal succeeded on 23 December 2020 that the extradition matter should revert to the Cape Town Magistrates' Court.[23] The concern here is

---

17 Anthony Valcke, 'The Rule of Law: Its Origins and Meanings (A short guide for practitioners)' (1 March 2012) <http://ssrn.com/abstract=2042336> accessed 14 April 2020 refers to 'The rule of law is traced to the expression of Professor AV Dicey, in 1885, and even as far back as Aristotle. Professor Dicey, back then said that when we speak of the "Rule of Law", as a characteristic of our country, "not only that with us no man is above the law, but that here, everyman, whatever his rank or condition, is subject to the ordinary law of the realm and amenable to the jurisdiction of the ordinary Tribunals'. The Laws (circa 360 B.C.) Dr Thomas Fuller in 1733 said 'Be you never so high, the law is above you.'

18 Valcke, 'The Rule of Law'.

19 Bingham, *The rule of law* 9.

20 *Mackeson v Minister of Information, Immigration and Tourism* [1980] (1) SA 747 (ZR) at 753-7.

21 Ramjathan-Keogh, 'South Africa, Apartheid, Crimes against humanity and the Rule of Law'.

22 *Kouwenhoven v Minister of Police* (1477/2018) [2019] ZAWCHC 154; [2019] 4 All SA 768 (WCC) (19 September 2019); K Evanoff and M Roberts, 'A sputnik moment for artificial intelligence geopolitics' *The Internationalist* (7 September 2017).

23 *Director* of *Public Prosecutions*, *Western Cape v Kouwenhoven* (A181/2020) [2020] ZAWCHC 185 *(*23 December 2020*)*. See also *Kouwenhoven v DPP (Western Cape) and Others* (288/2021) [2021] ZASCA 120 (22 September 2021).

whether or not these cases may create a defence to others who will oppose an extradition as a point in *limine*, that there are some persons who are exempt because of status or preference.

Cybercriminals target South Africa,[24] because they are aware of the difficulty of investigations regarding digital evidence and prosecutions, and which is even more difficult in cases involving extradition or mutual legal assistance request for cybersecurity transgressions. This remains a problematic issue, not only within the borders of SA, but internationally as well because the Cybercrimes Act is not fully in operation, and there is no certainty when the cybersecurity legislation will be passed. There can be no extradition if it contradicts the rule of law, in that no person is above the law. The maxim of *nulla poena sine lege*, is given meaning in the constitution, that the Republic of South Africa is one, sovereign, democratic state founded on Supremacy of the constitution and the rule of law.[25]

5.2.2 No prosecutions

In the absence of adequate cybersecurity legislation, further anomalies rise. There can be no prosecutions as there is no offence, and individuals live freely without fear[26] of criminal charges or extraditions. Interestingly, when the data breach occurred at Experian, consisting of identity numbers, phone numbers, physical and email addresses was first revealed to the public, Experian was

---

24 Business Insider SA 'Hackers on the dark web love South Africa - here's why we suffer 577 attacks per hour' (3 June 2020) <https://www.businessinsider.co.za/sa-third-highest number-of-cybercrime-victims-2020-6> accessed 5 June 2020.

25 Constitution, s 9 refers to Equality and reads:
'(1) Everyone is equal before the law and has the right to equal protection and benefit of the law.
(2) Equality includes the full and equal enjoyment of all rights and freedoms. To promote the achievement of equality, legislative and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination may be taken.
(3) The state may not unfairly discriminate directly or indirectly against anyone on one or more grounds, including race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth.
(4) No person may unfairly discriminate directly or indirectly against anyone on one or more grounds in terms of subsection (3). National legislation must be enacted to prevent or prohibit unfair discrimination.
(5) Discrimination on one or more of the grounds listed in subsection (3) is unfair unless it is established that the discrimination is fair.'

26 Mujuzi, 'The South African International Co-Operation in Criminal Matters Act' 351.

quick to point out that the data was harmless.[27] The Cybercrimes Act is not yet in full operation and not retrospective, therefore there can be no offence of theft, as the definition of 'theft in common law' excludes theft of incorporeal property.[28] The UK's Network and Information Systems Regulations (NISR)[29] establishes some legal protocols that ensure that selected digital service providers and essential services put into effect, sufficient measures to defend and improve the security of their network and information systems, focuses particularly on those services whose disruption, entail potentially significant damage to the UK's economy, its society and to ensure serious incidents are promptly reported to the competent authorities.[30] South Africa does not have similar legislation. In 2015 government responded with a National Cybersecurity Policy Framework (NCPF),[31] which is still a long way from being passed.

In 2019, South Africa had the third-highest number of cybercrime victims, of any country.[32] There were 577 hourly malware attacks, and malicious software paralysed the city of Johannesburg's power systems, with a demand for ransom in bit coin from some clan called the 'Shadow Kill Hackers'.[33] Hackers are savvy, skilful, ear marking South African people and businesses in premeditated attacks causing not only huge monetary losses but also loss of reputation.[34] The Coronavirus pandemic aggravated the number of attacks with a recorded 75% increase in instances of impersonation fraud in South Africa.[35] It still remains to be seen whether or not there will be any prosecutions emanating locally or internationally for the theft of personal data of twenty-four million South Africans and eight hundred thousand businesses potentially exposed to

---

27 Brian Pinnock, 'What recent data breaches tell us about cybersecurity in South Africa' *BusinessTech* (16 September 2020) <https://businesstech.co.za/news/industry-news/433797/what-recentdata-breaches-tell-us-about-cybersecurity-in-south-africa/> accessed 30 September 2020. See also G Hosken, 'Millions in SA at risk after data theft' *Sunday Times* (South Africa, 13 September 2020).

28 Cyber Crimes Act 19 of 2020.

29 UK Statutory Instruments 2018 No 506 (Network and Information Systems Regulations 2018) (NISR).

30 NISR 2018 No 506 – Explanatory note para 2.

31 Sutherland, 'Governance of cybersecurity' 83.

32 Business Insider SA, 'Hackers on the dark web love South Africa'.

33 BBC News 'Ransomware hits Johannesburg electricity supply' (26 July 2019) <https://www.bbc.com/news/technology-49125853> accessed 5 June 2020.

34 Pinnock, 'What recent data breaches tell us about cybersecurity in South Africa'.

35 Pinnock, 'What recent data breaches tell us about cybersecurity in South Africa'.

online fraudsters.[36] Experian confirmed that user data was transferred to a Swiss Company and uploaded to the company's system. The Swiss company's Chief Executive Officer blamed the Experian invasion on a Russian attacker.[37] President Putin made an interesting comment when he said, 'Never. Never. Russia does not extradite citizens to anyone.'[38] Article 14.6(*a*) of the African Union (AU) Convention on Cyber-Security and Personal Data Protection[39] states that data controllers 'shall not transfer personal data', to States outside the AU unless the State of the recipient 'ensures an adequate level of protection'.[40] It will be interesting to see if this catches the attention of the AU and if there are any prosecutions.

5.2.3 No procedures and RICA inconsistency with the Constitution

There are no procedures prescribed for certain offences in RICA.[41] This was also one of the reasons why RICA, was criticised with sections 35 and 37, being declared inconsistent and null because of; the failure to stipulate and list correct policies in directing government officials on how to deal with the intelligence extracted from interceptions.[42] The problem was also with collation of evidence and investigations. The court in the case of '*AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services*' looked at whether there were lawful grounds for the conducting of mass surveillance by the state.[43] The Court found that the processing of mass

---

36 Hosken, 'Millions in SA at risk after data theft'.

37 Hosken, 'Millions in SA at risk after data theft'.

38 Christopher Burgess, 'Do cybercriminals ever get extradited?' Security Boulevard (13 April 2018) <https://securityboulevard.com/2018/04/do-cybercriminals-ever-get-extradited> accessed 14 September 2020.

39 AU, 'Convention on Cyber-security and Personal Data Protection' (27 July 2014) <https://au.int/sites/default/files/treaties/29560-treaty-0048__african_union_convention_on_cyber_se curity_and_personal_data_protection_e.pdf> accessed 6 June 2020.

40 G Greenleaf and M Georges, 'The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?' (2014) 131 Privacy Laws and Business International Report 18-21.

41 No procedures prescribed for the Powers, functions and duties of Director in terms of s 35, Act 70 of 2002.

42 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC 03 [3]; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021).

43 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC 03 [3]; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) [4]. The High Court accepted the following

interception in communications was unlawful including overseas signal interception.[44]

5.2.4 Prescription and extradition

The issue of prescription can be raised as a defence in an extradition enquiry.[45] Section 18 of the Criminal Procedure Act[46] entails that that the State may and should not institute criminal proceedings against a suspected person after twenty (20) years from the date on which the transgression was committed. However, there are limitations. This section does not refer to extraditions and this issue may depend on the Treaty. An example is the treaty between the Republic of South Africa and the Argentine Republic which states that the prosecution for the offence or punishment for the requested extradition, would be prohibited by prescription under the protocols of the Requesting State.[47] However, it does not refer to the requested State. If South Arica was to extradite

---

explanation around bulk surveillance, which was provided by the respondents: 'Bulk surveillance is an internationally accepted method of strategically monitoring transnational signals, in order to screen them for certain cue words or key phrases. The national security objective is to ensure that the State is secured against transnational threats. It is basically done through the tapping and recording of transnational signals, including, in some cases, undersea fibre optic cables.'
'[I]ntelligence obtained from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals. It also includes any communication that emanates from outside the borders of [South Africa] and passes through or ends in [South Africa].'

44 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC 03 [3]; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) [4].

45 *Bell v State* A101/2014 ZAGPHC, unreported *S v Elran Meir*, case no 3/5403/13, Randburg Magistrates Court 13.

46 Act 51 of 1977. A special plea of prescription can be averred if the offence committed over 20 years, and the State would be barred from continuing with the charge but are not an absolute defence against all charges. The section makes provisions for specific exceptions for serious crimes which can still be prosecuted at any time after the 20-year period from date of incident has lapsed. These crimes include for example, Murder, Treason committed when the Republic is in a state of war, Aggravated robbery, Kidnapping, Child-stealing, Rape or compelled rape, Genocide, crimes against humanity and war crimes, Crimes and involvement in human trafficking, Trafficking in persons for sexual purposes, using a child or person who is mentally disabled for pornographic purposes and Torture.

47 GN 519 in *GG* 40978 of 14 July 2017 (Extradition Treaty Between the Republic of South Africa and the Argentine Republic, article 3(4)).

a fugitive to the Argentine Republic, and the offence was prescribed in South Africa, this would then be contrary to the principle of double criminality, or the rule of law by virtue of prescription. The concern is that there could be a stay of prosecution.[48]

5.3 *Aut dedere aut judicare*: Extradite or prosecute – the case of *S v Okah*

5.3.1 S v Henry Emomotimi Okah

In the above cited case, the facts were that Mr Okah,[49] was a Nigerian national residing in South Africa. He was prosecuted for terrorism related offence in terms of the 'Protection of Constitutional Democracy against Terrorist and Related Activities Act'.[50] (Act), in respect of two car bombings in which explosives were successively detonated in Warri, Nigeria on 15 March 2010, and double car bombings six months later in Abuja, Nigeria on 1 October 2010. There were extensive injuries and damage in both bombings.[51] Consequently, the prosecution in the Johannesburg High Court proved that the accused was the mastermind who funded the crimes, and he was convicted on all charges, however, the 'Supreme Court of Appeal' (SCA), exonerated him on four of the indictments.[52] The SCA made the distinction of the Accused occupancy or residence at the planning and execution of both the bombings.[53] The SCA's reasoning was that there was founding of partial jurisdiction only, created by the statute for deeds perpetrated beyond South African borders.[54]

---

48 Murdoch Watney, 'Unreasonable delays in criminal trials and the remedy of a permanent stay of prosecution *Zanner v Director of Public Prosecutions, Johannesburg* 2006 (2) SACR 45 (SCA)' (2007) 45 TSAR 422.

49 *S v Okah* (CCT 315/16; CCT 193/17) [2018] ZACC 3; 2018 (4) BCLR 456 (CC*); 2018 (4)* BCLR 456 (CC); 2018 (1) SACR 492 (CC) (23 February 2018) para 1 (hereinafter referred to the *Okah* case).

50 Act 33 of 2004.

51 *Okah* case [1] 'One person was killed in the Warri bombings, and at least eight people were killed in the Abuja bombings.'

52 *Okah* case [2] referred to High Court judgment.

53 *Okah* case [2] refers to Supreme Court of Appeal judgment - at paras 11 and 13.

54 The result was that the Supreme Court of Appeal replaced the sentence of 24 years' imprisonment the High Court imposed with a sentence of 20 years.

5.3.2 Extra-territorial jurisdiction of South African courts under 'Section 15(1) of the Act'

The court noted further the issue of whether South African courts have jurisdiction under section 15(1) of the Act to try alleged offences beyond the financing of an offence that occurred outside South Africa.[55] The Court noted that 'section 15(1)' is the principle constituent for jurisdiction of criminal acts of terrorism perpetrated abroad.[56]

This provision grants exoteric powers to South African courts relating to a 'specified offence' as prescribed.[57] The SCA confirmed the 'extra-territorial jurisdiction' of the courts in terms of the aforesaid section specifically for crimes related to financing of offences,[58] but the Constitutional Court found that the SCA's narrow interpretation creates a series of absurdities.[59] The provision has

---

55 *Okah* case [4].

56 *Okah* case [37]. Section 15(1) of Act 33 of 2004 provides: 'A court of the Republic has jurisdiction in respect of any specified offence as defined in paragraph (*a*) of the definition of 'specified offence', if—
- (*a*) the accused was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic; or
- (*b*) the offence was committed—
  - (i) in the territory of the Republic;
  - (ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed;
  - (iii) by a citizen of the Republic or a person ordinarily resident in the Republic;
  - (iv) against the Republic, a citizen of the Republic or a person ordinarily resident in the Republic;
  - (v) on board an aircraft in respect of which the operator is licensed in terms of the Air Services Licensing Act, 1990 (Act 115 of 1990), or the International Air Services Act, 1993 (Act 60 of 1993);
  - (vi) against a government facility of the Republic abroad, including an embassy or other diplomatic or consular premises, or any other property of the Republic;
  - (vii) when during its commission, a national of the Republic is seized, threatened, injured or killed;
  - (viii) in an attempt to compel the Republic to do or to abstain or to refrain from doing any act; or
- (*c*) the evidence reveals any other basis recognised by law.'

57 ' "Specified offence", with reference to Section 4, 14 (in so far as it relates to Section 4), and 23, means—
- (*a*) the offence of terrorism referred to in Section 2, an offence associated or connected with terrorist activities referred to in Section 3, a Convention offence, or an offence referred to in Section 13 or 14 (in so far as it relates to the aforementioned sections); or
- (*b*) any activity outside the Republic which constitutes an offence under the law of another state and which would have constituted an offence referred to in paragraph (*a*), had that activity taken place in the Republic.'

58 *Okah* case [14] - The Court overturned the Warri convictions.

59 *Okah* case [25].

the effect of a 'residual jurisdiction-granting clause',[60] and stipulating that any act alleged to constitute an offence committed by a person not contemplated by section 15(1) could nonetheless be brought in our courts provided that there is a particular nexus between the act or person and the country (South Africa). The court also criticized the SCA for the absurdities.[61] The court stated that the general obligation curtail terrorism is expansive and demands a reading of the Act as enabling South Africa to be involved, as a member of the international community, in the fight against an international and transnational phenomenon.[62] The apparent outcome of the debatable interpretation is that it would render the Act ineffective in its intended purpose to strengthen,[63] resulting in upholding the State's appeal, which set aside the SCA order. The point that looms large here, is that the prosecution was successful and the

---

60 Section 15(2) of Act 33 of 2004 provides:
'Any act alleged to constitute an offence under this Act and which is committed outside the Republic by a person other than a person contemplated in Subsection (1), shall, regardless of whether or not the act constitutes an offence or not at the place of its commission, be deemed to have been committed also in the Republic if that—
(*a*) act affects or is intended to affect a public body, any person or business in the Republic;
(*b*) person is found to be in the Republic; and
(*c*) person is for one or other reason not extradited by the Republic or if there is no application to extradite that person.'

61 Paragraph 26 of the Judgment - Section 11, makes it a crime to harbour a person 'who has committed a specified offence' and the SCA's interpretation of 'specified offence', would mean that a court has no jurisdiction to try someone for harbouring a terrorist, but it would have jurisdiction to try someone for harbouring a terrorist-financier.
Paragraph 27 - Second, the Supreme Court of Appeal's interpretation radically and absurdly restricts Section 4.
Paragraph 28. Third, the Supreme Court of Appeal's approach fails to explain how Section 23 – which is one of the provisions implicated 'with reference to' – could limit the definition of a specified offence.
Paragraph 29 - The Supreme Court of Appeal's interpretation overlooks the fact that Section 23 is included in the list of provisions 'with reference to' which 'specified offence' is defined.
Section 23 is titled 'Freezing order'. It provides:
(1) A High Court may, on ex parte application by the National Director to a judge in chambers, make an order prohibiting any person from engaging in any conduct, or obliging any person to cease any conduct, concerning property in respect of which there are reasonable grounds to believe that the property is owned or controlled by or on behalf of, or at the direction of—
(*a*) any entity which has committed, attempted to commit, participated in or facilitated the commission of a specified offence; or
(2) An order made under subsection (1) may include an order to freeze any such property.'
Okah case. Another absurd result would be that courts would be able to make Section 23 freezing orders only in relation to financing offences but not in relation to the offence of terrorism.

62 *Okah* case [36].

63 *Okah* case [36].

Protection of Constitutional Democracy against Terrorism and Related Activities Act[64] withstood the constitutional challenges of extra territorial jurisdiction. This case paves the way for extra-territorial jurisdiction prosecutions regarding the Cybercrimes Act.[65]

5.4 Mutual legal assistance (MLA) as an effective measure of cybercrime

5.4.1 Challenges of mutual legal assistance

The Cybercrime Convention Committee (T-CY) undertook a detailed evaluation with thirty-six Parties and three Observer States (South Africa excluded) on how mutual legal assistance functioned, by focusing on Article 31 of the Budapest Convention.[66] Article 31[67] refers to mutual assistance regarding accessing stored computer data for the rendering of international cooperation more efficiently. South Africa is party to the convention but has not yet ratified the treaty.[68] The Budapest Convention seeks to promote international cooperation on cybercrime. Legislation that aligned with the convention ensures countries have harmonised and compatible legislation that is not identical in the context of cybercrime legislation.[69] No African country has ratified the treaty and dual

---

64 Act 33 of 2004.

65 Act 19 of 2020.

66 T-CY Assessment Report.

67 European Convention on Cybercrime, 'Budapest, 23.X1.2001 European Treaty Series - No 185.

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.
2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
3. The request shall be responded to on an expedited basis where:
   a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
   b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

68 T-CY Assessment Report. In signing the Protocol, States only indicated general support for its objective and provisions as well as their intention to become Parties in the future and be legally bound by it. However, the act of signing, in itself, did not establish consent to be bound by the Protocol. Therefore, the further act of ratification is required before the State becomes a Party; Ratification of Accession (4 June 2001) <https://bch.cbd.int/help/topics/en/Ratification%20and%20Accession.html> accessed 14 May 2020.

69 Dennis Mbuvi, 'African States Urged to Ratify Budapest Cybercrime Convention' (10 October 2011) <https://www.csoonline.com/article/2129762/african-states-urged-to-ratify-buda pest-cybercrime-convention.html> accessed 13 January 2021.

criminality is required for countries to exchange cybercrime information linked to cybercrime.[70]

The T-CY Committee found amongst other findings:

i) Mutual assistance in relation to access to information stored did not only hinge on offenses detailed on the computers. Fraud was found to be most common, including the different kinds of fraud as well as transgressions relating to computer systems, unlawful ingress and interference, circulation of harmful software and information.[71]

ii) The responses in the study imply that legal assistance is viewed as rather complicated, protracted and costly in procuring digital proof; and therefore, it is not usually continued. Agencies are inclined to seek evidence *via* police cooperation when avoiding MLA in spite of the fact that the evidence gathered cannot be used in many instances, and often investigations are abandoned.[72]

iii) 'Article 26 of the Budapest Convention' relating to the sending of 'spontaneous' intelligence,[73] is underused. It can lead to multi-country operations as well as providing important data for interrogation of sophisticated crimes including racketeering.[74]

iv) Some States refuse cooperation if the case is viewed as minor or entails excessive investigation burdens on authorities, although the so-called small matters could be a lead to the bigger cases involving nefarious

---

70 Mbuvi, 'African States Urged to Ratify Budapest Cybercrime Convention'.

71 T-CY Assessment Report 5.

72 T-CY Assessment Report 7.

73 European Convention on Cybercrime, European Convention on Cybercrime, 'Budapest, 23.X1.2001 European Treaty Series - No 185', Article 26 – Spontaneous information:

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

74 T-CY Assessment Report 9-10.

consortiums.[75] Dual criminality is generally a requirement for mutual legal assistance in seeking and applying for saved or gathered computer information. Parties are encouraged to apply less rigidity in the application of double criminality, particularly to transgressions under 'Articles 2 to 11 of the Budapest Convention'.[76]

The Committee also found several problems, amongst others relating to MLA requests, namely time, workload and the complexity; delays in responding to a request; refusal to cooperate; non-compliance to dual criminality requirements, and limited technological skills.[77]

The same States that belong to the Budapest treaty are also members to the European treaty on 'Cooperation in Criminal Matters treaty',[78] with twenty-eight of them also being parties to the 2nd addition to the 'ETS 182' treaty. One of the features of this agreement is that it permits the immediate cooperation within judicial offices.[79] Since South Africa is only a signatory, international cooperation and urgency most probably will be ineffective or lost. Alexander Seger, head of COE's cybercrime division pronounced on countries that have become a signatory or party to the treaty, have been able to mobilise

---

75 T-CY Assessment Report 34.

76 European Convention on Cybercrime, 'Budapest, 23.X1.2001 European Treaty Series - No 185'; Council of Europe, 'Explanatory Report to the Convention on Cybercrime (European Treaty Series No 185)' 259.

77 T-CY Assessment Report 38-40.
i) Time, workload and the complexity of procedures required to prepare or execute MLA,
ii) The delays of six to twenty-four months in response to requests in general,
iii) Refusal to cooperate or no reply from some countries,
iv) The problem of cooperation with 24/7 contact points,
v) No receipt that MLA request has been received or that data has been preserved,
vi) Legal restrictions (data protection),
vii) Dual criminality requirement not met,
viii) MLA request not preceded by preservation request to ensure that data is still available,
ix) Overburdened by too many requests,
x) Limited technical skills and understanding regarding electronic evidence requested.

78 European Treaty Series – No 30.

79 European Treaty Series – No 30' December 2020; ETS 182, a 4 - Channels of communication. 'Requests for mutual assistance, as well as spontaneous information, shall be addressed in writing by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party and shall be returned through the same channels. However, they may be forwarded directly by the judicial authorities of the requesting Party to the judicial authorities of the requested Party.'

technical assistance.[80] Article 25.3 of the Budapest convention allows for expedited means of communication in urgent circumstances.[81]

5.4.2 Transborder effectiveness in respect of cybercrimes

Unlike offline offences, there is evidently no crime scene online or cyberspace, in the conventional context of finding evidence such as fingerprints, DNA or, or interviewing witnesses.[82] The offences are 'committed without climbing over fences, balaclavas or angry dogs and property owners and somewhere in the world, where there is a computer which is controlled by a particular person'.[83] The exercise of jurisdiction in the context of cybercrimes, remains largely based on the principle of territoriality, which renders it difficult to pinpoint any particular location where the cybercrime occurred. Such difficulty is by legal and technical challenges[84] in determining the physical location of the place at which the cybercrime originates. It appears merely in identifying the Internet Protocol (IP) address of the computer system used by the cybercriminal.[85] There is, however, a range of techniques, software programs and website paths to conceal their true IP address and the place of the criminal conduct.[86]

Article 32[87] has been criticized[88] for the following reasons:

---

80 Mbuvi, 'African States Urged to Ratify Budapest Cybercrime Convention'.

81 European Convention on Cybercrime, 'Budapest, 23.X1.2001 European Treaty Series - No 185', Article 25.3 'Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.'

82 AMG Smit, 'Criminal law on cyber crime in the Netherlands' (Preparatory Colloquium Helsinki (Finland), 10-12 June 2013. Section IV: International Criminal Law) <http://www.pe nal.org/sites/default/files/files/RH-11.pdf> accessed 15 January 2020.

83 Smit, 'Criminal law on cyber crime in the Netherlands'.

84 Jean B Maillart, 'The limits of subjective territorial jurisdiction in the context of cybercrime' (2014) 40 ERA Forum 375.

85 Maillart, 'The limits of subjective territorial jurisdiction' 379.

86 Maillart, 'The limits of subjective territorial jurisdiction' 379.

87 European Convention on Cybercrime, 'Budapest, 23.X1.2001 European Treaty Series - No 185'.
'Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party:
a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the

i. Transborder searches are not covered by the Convention,

ii. On a plain reading it appears that permission is required for liaisons with Law Enforcement Agencies of a particular State and citizens of a foreign country. This assistance with requests and providing for information could be both a violation and crime of the sovereignty of a State.

iii. The contentions are that Article '32(*b*)' requires the consent of an individual that falls under the investigating jurisdiction.[89]

Article 32 evades using mutual legal assistance protocols and is regarded as contentious and most probably is a reason why Russia[90] is not ratifying the Convention.

5.4.3 The complexity of transborder 'access to data and jurisdiction'

The report on cross-border data and territorial access[91] underpins the necessity for cross-border accession but highlighted issues and dangers (both licit and policy considerations, including safeguards for non-public information and implementation of the law) that should be dealt with if transborder laws were to be supplemented, then there must be further protective measures.[92] The report further highlighted that the Budapest treaty prohibits 'blanket/mass transborder access, collection or transfer of data'.[93] In the interesting case of '*Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium*, No ME20.F1.105151-12 of 27 October 2016'; unveils how the Belgium court

---

person who has the lawful authority to disclose the data to the Party through that computer system.'

88 Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation Cybercrime' (2014) 40 Monash University Law Review 698.

89 European Treaty Series No 185 60, 294.

90 Computer Crime Research Center, 'Putin Defies Convention on Cybercrime' (28 March 2008) <https://www.crime-research.org/news/28.03.2008/3277/> accessed 15 January 2021.

91 T-CY Assessment Report.

92 T-CY Assessment Report.

93 T-CY Assessment Report para 2.1.1.

established jurisdiction[94] and directed the registration and surveillance of an alleged perpetrator's Skype address. The accused was located in Luxembourg. Therefore, any information external to wilful disclosure compliance would have to be requested via MLA. It was then argued that a Belgian judge had no jurisdiction.[95] The court found the offender to have freely presented himself as a service supplier in the Belgian market and vital to comply with Belgian law, compelling the authorities to render technological cooperation on request.[96]

5.5 Conclusion

The global problem remains in spite of international efforts to address information technology and cybercrime, which is still limited and remains reactive regardless of technology transformation.[97] The Convention on Cybercrime[98] appears to be the only substantive multilateral agreement addressing cybercrime with convergent, harmonised legislation and capability secbuilding.[99] The Cybercrimes Act is not fully in operation but does create new cyber offences; however there were many criticisms with the Bill. Currently, extraditions relating to cybersecurity offences may be challenging,[100] and SA may not be able to extradite a foreign national nor prosecute the person.

In terms of the *aut dedere aut judicare* principle applies where a state refuses to extradite its own citizens, and it is suggested that where there is a conviction,

---

94 EUROJUST, 'Cybercrime Judicial Monitor' para 3.1 Selected Court Rulings at 13 (Court of First Instance Antwerp, Section Mechelen, ME20.F1.105151-12, Belgium, 27 October 2016) (December 2017) <https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2017-12_CJM-3_EN.pdf> *Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium,* No. ME20.F1.105151-12 of 27 October 2016 accessed 25 May 2020.

95 EUROJUST, 'Cybercrime Judicial Monitor' para 3.1 Selected Court Rulings at 11.

96 EUROJUST, 'Cybercrime Judicial Monitor' para 3.1 Selected Court Rulings at 14. The Court of Appeal in Antwerp confirmed the judgement of the Court of First Instance and referred to the case of *Inc v UEJF and LICRA* USA001R.

97 Evanoff and Roberts, 'A sputnik moment for artificial intelligence geopolitics'.

98 European Convention on Cybercrime, 'Budapest, 23.X1.2001 European Treaty Series - No 185'.

99 DA Patel and S Bharadwaj, 'Budapest Convention on Cyber Crime' (2020) <http://studymaterial.unipune.ac.in:8080/jspui/bitstream/123456789/4798/1/BUDAPEST%20CONVENTION%20ON%20CYBER%20CRIME-converted.pdf> accessed 26 May 2020.

100 Pinnock, 'What recent data breaches tell us about cybersecurity in South Africa'. See also Hosken, 'Millions in SA at risk after data theft'. 'The local data breaches coincided with high profile attacks and outages for global brands like Twitter and Garmin. And in headline-grabbing news, credit bureau Experian reported a massive breach of data that exposed the personal information of up to 24 million South Africans and nearly 800,000 businesses.'

then the person be repatriated for sentencing.[101] This approach would recognise the territorial state for trial and the home state for punishment and rehabilitation.[102] Irregular rendition and abduction is an undesirable alternative.[103] Traditionally, jurisdiction was restricted to crimes in a particular state's territory and international conventions on terrorism have justifiably relaxed such restrictions,[104] territoriality was the conventional base for establishing jurisdiction, such as South African jurisprudence also recognise other methods of asserting jurisdiction.[105] The Court had reason to analyse the 'Protection of Constitutional Democracy against Terrorist and Related Activities Act',[106] because of the '*aut dedere aut judicare'* doctrine.

The definition of 'specified offence' was analysed in depth, and the court found it to be vital in terrorism crimes.[107] Sections 1 and 2[108] must be read together as they are intertwined with 'terrorist activity', transgressions, and granting cross border authority referred to in 'Section 15'.[109] South Africa has international obligations not only to fight terrorism but also to try criminals and extradite them, irrespective of who they may be.[110] There are international frameworks establishing the twin duties, for example, the UN Security Council resolution.[111] 'Section 233 of the Constitution' necessitates that the Court interprets the Act[112] in tandem with international jurisprudence, and requiring that South Africa actually prosecutes or extradites individuals similar to Mr Okah.[113] Comity

---

101 Watney, 'A South African perspective on mutual legal assistance' 306.

102 Boister, 'The trend to "universal extradition"' 299-300.

103 Boister, 'The trend to "universal extradition"' 300; see also, *S v Ebrahim* (279/89) [1991] ZASCA 3; 1991 (2) SA 553 (AD); [1991] 4 All SA 356 (AD) (26 February 1991).

104 *Okah* case [41].

105 *Okah* case [42]. See also *S v Basson* [2005] ZACC 10; 2007 (3) SA 582 (CC); 2005 (12) BCLR 1192 (CC) at paras 223-225.

106 Act 33 of 2004.

107 *Okah* case [31].

108 Act 33 of 2004.

109 *Okah* case [32].

110 *Okah* case [35].

111 *Okah* case [35]. The preamble of Act acknowledges UN Security Council Resolution 1373/2001 as binding on all Member States. UN Security Council Resolution 1373/2001 requires that states shall—
'[E]nsure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts.'

112 Act 33 of 2004.

113 *Okah* case [37].

concerns do not apply in cases where jurisdictional infringement of another State has not occurred.[114]

The 'Cybercrime Convention Committee (T-CY)'[115] evaluation found that MLA was regarded as convoluted, protracted and costly to gather electronic data, and frequently given up. Since South Africa is only a signatory to the Cybercrime Convention, international cooperation and urgency could probably be ineffective or go astray. Alexander Seger proffered that signatory countries or parties to the treaty were able to canvass or source technical assistance[116] which would be effective for investigations, especially with the complexity of transborder access to data and jurisdiction.[117] The report on the transborder access to data and jurisdiction underlined the need for transborder access.

South Africa has assented on the 6 November 1996 to the International Co-Operation in Criminal Matters[118] (ICCM), 'to facilitate the provision of evidence, the execution of sentences, the confiscation and transfer of the proceeds of crime between SA and foreign States'. The ICCM regulates the law in respect of mutual legal assistance.[119] Section 2(2) appears to be onerous, and rigid with the potential failed application.[120] The criticism is that section 7 of the ICCM should follow the Namibian International Co-operation in Criminal Matters Act 9 of 2000 (ICCMA), which is more flexible and accommodating in urgent situations especially in regard to electronic crimes.[121] The ICCM make provisions for mutual assistance to enforce orders

---

114 *Okah* case [42].
115 T-CY Assessment Report.
116 Mbuvi, 'African States Urged to Ratify Budapest Cybercrime Convention'.
117 T-CY Assessment Report.
118 International Co-operation in Criminal Matters Act 75 or 1996.
119 Watney, 'A South African perspective on mutual legal assistance' 292.
120 Act 75 or 1996, s 2(2) 'A judge in chambers or a magistrate may on application made to him or her issue a letter of request in which assistance from a foreign State is sought to obtain such information as is stated in the letter of request for use in an investigation related to an alleged offence if he or she is satisfied-
(*a*) that there are reasonable grounds for believing that an offence has been committed in the Republic or that it is necessary to determine whether an offence has been committed;
(*b*) that an investigation in respect thereof is being conducted; and that for purposes of the investigation it is necessary in the interests
(*c*) of justice that information be obtained from a person or authority in a foreign State.'
121 Mujuzi, 'The South African International Co-Operation in Criminal Matters Act' 351.

pertaining to criminal proceedings but no provision exist for implementing prison sentences in South Africa.[122]

The following chapter provides a framework of conclusions and recommendations based on the core tenets.

[122] Watney, 'A South African perspective on mutual legal assistance' 295.

Chapter 6: Conclusions and recommendations

6.1 Introduction

In this study the question is: how does cybercrimes impact on extradition?[1] Some of the cyber laws in South Africa were discussed with the various relevant pieces of the regulations and penalties.[2] The Cybercrimes Act repeals certain acts and sections, aiming to achieve unification and codification of computer crimes.[3] The study aims to determine whether or not our cyber laws and treaties relating to cybercrime do in fact promote or negatively affect extradition as well as the issue of double criminality. To answer this question, the study was segmented in that Chapter 2 addressed the extraditions and the requirement of dual criminality. Our case law confirms the applicability of the double criminality principle of the extradition request, which is a departure from the United Kingdom practise.[4] The rule of law is trite, and there can be no violation in the event that there is no law.[5] The effect is that there may be no extraditable offence,[6] which in turn has the effect that until the Cybercrimes Act comes into full operation or cybersecurity legislation is passed, an extradition request relating to specific requests may remain latent, or not processed. The issue of transnational cybercrime creates systemic risk not only to South Africa but to foreign States as well.

6.2 Summary of discussions, findings and recommendations

6.2.1 South African extradition jurisprudence

6.2.1.1 Summary

South Africa's extradition procedure is regulated by the Extradition Act 67 of 1962.[7] The United Nations Model Treaty provides a 'useful framework' for negotiating and revising bilateral extradition agreements.[8] Double criminality principle is a substantive requirement for extradition based on the reciprocity of

---

1 Section 1.3.1.
2 Section 3.
3 Section 3.3.
4 Section 2.3.4.
5 Section 5.2.1.
6 Section 2.2.3.
7 Section 2.1.
8 Section 2.1.

similar mutual treatment deriving from the mutuality of legal obligations.[9] Such reciprocity requires one conduct be based on an extraditable will constitute criminal transgression in both the requested and the requesting State.[10] Extradition proceedings are sui generis in nature,[11] and the process thereof comprises bilateral agreement between two sovereign States relating to the surrender of individual in response to a request for extradition by the other (the requesting) State.[12]

International and domestic law governs the extradition process through diplomatic channels. Section 3 of the Extradition Act deals with extraditions, where the foreign authority has such agreement with this government. It also addresses a foreign jurisdiction that is not privy to an agreement of extradition, in which case the person shall still bear the liability to be surrendered, in the event that has so consented.[13] All persons in an extradition inquiry are entitled to apply for bail, and section 9 of the Extradition Act intimates that the magistrate must hold an inquiry with a purpose of a surrender relating to such person to the foreign State. A finding by a magistrate in terms of section 10 is made; that the evidence is sufficient to make the person liable to surrender however, subject to the discretion of Minister of Justice under section 11.[14]

The British Extradition Acts of 1870 to 1906 governed extradition arrangements between other Commonwealth countries and South Africa. The withdrawal of the latter country from the Commonwealth in 1961 gave rise to lapse of many of country's extradition treaties, resulting in the Extradition Act 67 of 1962 was enacted. South Africa has acceded to the multilateral European Convention on Extradition of 1957 and is presently a party with a further 50 states.[15] In the case of *Mohamed and Another v President of the Republic of South Africa and Others*,[16] the Constitutional Court intimated that the nature of extradition, involved three elements, namely the sovereignty of two States; a request for the delivery of an alleged criminal; and the resulted delivery of the person

---

9 Section 2.1.
10 Section 2.1.
11 Section 2.
12 Section 2.1.
13 Section 2.2.1.2.
14 Section 2.2.1.2.
15 Section 2.2.2.
16 Section 2.2.2.

requested. In *President of the Republic of South Africa and Others v Quagliani*,[17] the court acknowledged that extradition encompassed more than reciprocity or international. Section 2 of the Extradition Act empowers the President to establish extradition agreements with foreign jurisdiction, and requests for extraditions may be undertaken in the context of comity (the goodwill among states).[18]

Double criminality principle is central to laws pertaining to extradition.[19] Section 3(1) of the Extradition Act,[20] provides that any accused individual who is also convicted of the relevant offence in the treaty of agreement, shall be liable to be surrendered to such foreign jurisdiction. The extraditable offence and alleged conduct in the foreign jurisdiction must be a criminally punishable offence in South Africa,[21] with the sentence that is above a particular severity. Boister argues that the offence should also be recognised as extraditable by both states,[22] and serious enough to warrant a request for an extradition.[23]

The definition of Extradition relates to the delivery of a person by a State in whose territory he happens to be for that particular time to the state where he is accused or found guilty of a crime.[24] The guarantee of the delivery of the accused outside the borders of the requesting state is sometimes constitutes a problem. Our case law condemns law enforcement by kidnapping or entering the territory of another state to collect evidence as it is considered to be both, a transgression of international law,[25] and an infringement of the sovereignty of the state being entered.[26] Cooperation by mutual legal assistance[27] is therefore, encouraged.

Our case law has evolved in respect of the dual criminality principle. The matter of the time has been extensively dealt with by the courts, accruing from the interpretation of section 3 of the Extradition Act, in relation to whether or not the

---

17 Section 2.2.2.
18 Section 2.2.2.
19 Section 2.2.1.1.
20 Section 2.2.3.
21 Section 2.2.3.
22 Section 2.2.3.
23 Section 2.2.3.
24 Section 2.2.1.1.
25 Section 2.2.1.1.
26 Section 2.2.1.1.
27 Section 2.2.1.1.

extradition request should constitute a crime in South Africa, at the time when the request was made; or only at the time of the alleged offence. The definition of an extraditable offence[28] broadens the scope to transgression prior to the Extradition Act, and also before or after the date a bilateral agreement comes into operation. In between, the absence of legislation means there can be no extraditable offences, which is a right entrenched in section 35(3)[29] of the Constitution.[30] South African courts had to look to the UK case of *ex parte* Pinochet Ugarte[31] for guidance on the aspect of the time of the extradition request. The UK case involved a Chilean former head of state who was arrested in London through the instigation of a provisional warrant.[32] Six days later a second warrant was issued on receipt of a second international warrant of arrest issued by the Spanish court, in which it was alleged that the former Chilean head of State had ordered his subordinates to commit acts of torture in hostage taking during his tenure.[33] The Court quashed both warrants, and subsequent majority ruling on the re-hearing of the Appeal held that the alleged conduct should be crime in the United Kingdom law as well as the law of the requesting State (Chile).[34] It was a requirement that the alleged conduct should be a crime in the United Kingdom at the time of committing the alleged offence. The Applicant was not extradited.[35] However, the dissenting view firstly; did not support this finding, on the basis that there could be no immunity for torture committed in his official capacity as Head of state, as torture constituted an international transgression against humanity and jus cogens, because of the ratification of the convention whose signatories were Spain, Chile and the United Kingdom in 1988.[36]

The courts were to rule on this issue in the two cases of *Palazzolo v Minister of Justice and Constitutional Development*.[37] The court confirmed the *Pinochet Ugarte* case, that double criminality requires that the conduct should be an offence in both the countries at the time of the commission of the offence. The

---

28 Section 2.3.1.
29 Section 2.3.1.
30 Section 2.3.1.
31 Section 2.3.1.1.
32 Section 2.3.1.1.
33 Section 2.3.1.1.
34 Section 2.3.1.1.
35 Section 2.3.1.1.
36 Section 2.3.1.1.
37 Section 2.3.1.2.

Italian Government made six requests to the South African counterparts, over a period of two decades, for the extradition of the applicant (Palazzolo).[38] The court had pronounced on a conviction for the offence of aggravated Mafia-type Italian Criminal Code for the sentence of nine years imprisonment, was confirmed by the Appeal Court of Palermo and by the Supreme Court of Appeal in Rome. Mr Palazzolo, in-spite of being a fugitive, became a South African national by automatic naturalisation in 1995.[39] The finding of the Western Cape High Court did not show an extraditable offence in that that the conviction of a Mafia-type association under the Italian Criminal Code did not have corresponding reference in South African criminal law.[40] There could be no reliance on the Prevention of Organised Crime Act 121 of 1998 and the Prevention and Combating of Corrupt Activities Act 12 of 2004, as they were not promulgated at the time that the Applicant was allegedly involved in Mafia-type activities.[41]

The Randburg Court had to reconsider the issue of the time in the extradition request of Patel Usman Ismail.[42] The United States of America (USA) requested the extradition of Mr Patel from South Africa, for him to be prosecuted for banking-related offences in the USA between 2005 to October 2007. The corresponding charges in the RSA, would have been the Financial Intelligence Centre (FIC) Act 38 of 2001 which only came into operation in 2010, after the commission of the offences in the USA. The argument was that these offences were not yet offences in the Republic of South Africa at the time they were committed in the USA.[43] The magistrate interpreted section 3(1) of the Act[44] as encompassing transgressions committed before the existence of the Act, or before the conclusion of the treaty.[45] In *Bell v State*,[46] this case dealt with the extradition request by the Australian authority's charges that took place more than two decades previously committed in February 1977.[47]

---

38 Section 2.3.1.2.
39 Section 2.3.1.2.
40 Section 2.3.1.2.
41 Section 2.3.1.2.
42 Section 2.3.1.3.
43 Section 2.3.2.
44 Section 2.3.1.3.
45 Section 2.3.1.3.
46 Section 2.3.2.
47 Section 2.3.2.

The Eastern Cape Division held that transgressions committed more than twenty years previously, were not punishable and therefore, Bell's extradition request in respect of the offences were not extraditable offences, and further that at the time of the extradition enquiry there was no treaty between Australia and South Africa.[48] This case was criticized in that t*he court possibly went too far by unwittingly giving the definition of 'extraditable offence' in the Act.*[49] In the *Pinochet (No 3)* case, Lord Bingham CJ and Lord Lloyd were extolled for their decision, that their interpretation specifically date of the extradition requested, and not the date of the commission of the offence in the foreign State.[50] The SCA endorsed this finding, and came to the same conclusion in the *Patel* case.[51]

The definition of extraditable offences is contained in Article 2 of the Convention, which stipulates that the offense was punishable under the laws of the requesting and of the requested Party, with detention for a severity period of at least twelve months or even a more severe penalty.[52] If certain offences excludes an extradition in respect of the law of a Contracting Party, the Secretary-General should be informed to notify the other signatories.[53] The magistrate would have to look at the treaty itself for a determination on whether or not the offence is included. In the absence of a treaty, the magistrate must be satisfied that the said person is accused of an extraditable offence within the territorial jurisdiction of the foreign State, and sufficient detail of the offence must be placed before the magistrate for the proper determination.[54] Therefore, it would be proper section 10(2)[55] certificate be issued, in order to assist the magistrate insofar as the sufficient evidence to warrant a prosecution in the foreign State. The Constitutional Court[56] has already declared that a section 10(2) certificate is consistent with the Constitution.

---

48 Section 2.3.2.
49 Section 2.3.4.
50 Section 2.3.4.
51 Section 2.3.4.
52 Section 2.3.3.
53 Section 2.3.3.
54 Section 2.3.3.
55 Section 2.3.5.
56 Section 2.3.5.

6.2.1.2 Finding

The freedom of movement and trade in the cyber age creates not only devices for the perfect opportunity for globalization of culture and commerce, but also crime as well.[57] The pursuit of fugitives from justice to jurisdictions where they have committed no crime and do not face prosecution, have always been a concern for countries. The fleeing of individuals is also due to the porous international borders that made transnational flights easy.[58]

Section 1 of the South African Extradition Act refers to conduct which must constitute a crime in South African law and in the foreign state,[59] which is known as the principle of dual criminality. An extraditable offence has to be committed in order to succeed with an extradition request. An extradition request which must be communicated through diplomatic channels, with the supporting original documents or authenticated copies, including details of the offences and the relevant law.[60]

Dual criminality is interconnected with extraditable offences,[61] and this must be evident from both the Act and Treaty. The return of fugitives is generally secured by extradition agreements,[62] and the Extradition Act 67 of 1962 governs South Africa's extradition relations.[63] In terms of Article 2(1) of the European Convention on Extradition[64] the offence should be punishable under the laws of both the requested and the requesting party.[65] South Africa has to fulfil its international obligations where it is bound by an extradition treaty, and even a non-treaty extradition by[66] implementing or where such Extradition has been designated,[67] by the President. Self-executing treaties in terms of section 231(4) of the Constitution of RSA has drawn much jurisprudential interest.[68]

---

57 Section 2.5.
58 Section 2.5.
59 Section 2.5.
60 Section 2.5.
61 Section 2.5.
62 Section 2.5.
63 Section 2.5.
64 Section 2.5.
65 Section 2.5.
66 Section 2.5.
67 Section 2.5.
68 Section 2.4.

The Supreme Court of Appeal (SCA) in the *Patel* case has settled the issue of the double criminality rule by finding that the offence must exit at the date of the request for the extradition of a fugitive and not at the date the crime was committed in the state of the requesting party.[69] Section 18 of the Criminal Procedure Act refers to prescription of right to institute prosecution shall lapse after the expiration of a period of 20 years from the time of the commission of the offence but does not specifically refer to the time lapse in extraditions.[70] The issue of prescription in an extradition can be raised as point in *limine* or as a defence.[71]

The anomaly that arises is that some requests for cyber offences may remain pending until the Cybercrimes Act becomes wholly operational, or until cybersecurity legislation is enacted, to give effect to the dual criminality principle. This implies that there is no standard or prescription as to time the requesting State can bring an extradition request,[72] which was also the argument in the *Palazollo* case that a further extradition request would result in the arrest and in the infringement of the applicant's fundamental rights.[73]

The Constitutional court has declared section 5(1)(*a*) of the Extradition Act unconstitutional. The Magistrate can no longer issue a warrant of arrest for the surrender of a person upon a mere receipt of a notification by the Minister.[74]

6.2.2 A synopsis of legal precepts

6.2.2.1 South Africa's system of cyber laws

Chapter 3 deals with South Africa's cyber law and whether it matches up with international standards. Based on the fact that South Africa has a different regime of cybercrime legislation, namely: the common law, the Electronic Communications and Transactions Act (ECT Act),[75] the South African Police Service Act (SAPS Act),[76] Correctional Services Act,[77] the National Prosecuting

---

69 Section 2.5.
70 Section 2.4.
71 Section 2.4.
72 Section 2.4.
73 Section 2.4.
74 Section 2.5.
75 Section 3.1.
76 Section 3.1.
77 Section 3.1.

Authority Act,[78] Financial Intelligence Centre Act (FIC Act),[79] the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA),[80] South Africa's Protection of Personal Information Act (POPI Act),[81] and finally the Cybercrimes Act 19 of 2020. The Cybercrimes Act will repeal certain sections of the ECT Act relating to unauthorised computer access to data, extortion, fraud and forgery, attempt, aiding and abetting, that is sections 85, 86, 87, and 88.[82]

The prosecution relies on the common law offences of fraud by misrepresentation, in respect of identity theft, where a person may be found guilty of fraud, forgery, and uttering of a forged document, or alternately prosecuted in terms of section 18[83] of the Identification Act. The most common of cybercrime offences are identity theft, denial-of-service attacks[84] and hacking. The plague of identity theft in South Africa,[85] and the rise is due to superfluities of existing databases containing vital personal information, may render consumer protection[86] and the existing legislation inadequate.[87]

The Electronic Communications and Transactions Act,[88] is one of the sources of law which impacts on electronic communications and transactions, and also deals with issues which are not related to electronic communications and transactions. The Protection of Personal Information through electronic transactions only applies to personal information, cyber-identification and authentication still remains a risk.[89] Provision was made for the establishment of an Accreditation Authority that voluntary allows for the accreditation of an electronic signature.[90] The accreditation of authentication of services by the ECT Amendment Bill's is also to protect South African domain names,[91] prevent abuse of Information systems and secure worldwide electronic commerce.

---

78 Section 3.1.
79 Section 3.1.
80 Section 3.1.
81 Section 3.1.
82 Section 3.1.
83 Section 3.2.1.
84 Section 3.2.1.
85 Section 3.2.1.
86 Section 3.2.1.
87 Section 3.2.1.
88 Section 3.2.2.
89 Section 3.5.
90 Section 3.2.2.
91 Section 3.2.2.

Chapter XIII introduced statutory criminal offences relating to cybercrime, with the penalties of a fine or imprisonment for periods not exceeding 12 months or not exceeding five years.[92] These provisions will be repealed once the Cybercrimes Act comes into operation.

Section 71 of the South African Police Service Act makes it a criminal offence regarding unauthorised access and is broad to include all forms of access. In terms of subsection (2)[93] it refers to the wilful gaining of unauthorised access, program or data, with a penalty of a fine or imprisonment not exceeding two years. Subsection (3)[94] also has a similar penalty in respect of any person who wilfully performs an unauthorised function. Subsection 4,[95] refers to the wilful unauthorised modification that impairs the operation or program or operating system of any computer, with the penalty of a fine or imprisonment not exceeding five years. This reference to the word 'wilful', goes to intention and which maybe a difficult onus where there is negligence.[96] However, section 71 will be deleted once the Cybercrimes Act is in operation.

In terms of section 128 of the Correctional Services Act (CSA), deals with unauthorised access or modification of computer material under the control or in the custody of the Department or official. Subsection (1)(*b*) includes the physical components, and any program or data. Modification refers to both temporary or permanent as well as the circumstances regarding unauthorised access. Subsection (2)[97] refers to intentionally gaining unauthorised access, and not 'wilfully' as used in the SAPSA. The penalty is a fine or imprisonment for a period not exceeding two years or both. The intentional modification provisions are similar to subsection 71 of the SAPSA.[98] However, section 128 will also be deleted once the Cybercrimes Act is in operation.

The National Prosecuting Authority Act also refers to unauthorised access and specifies what is meant by unauthorised access. These are similar provisions to SAPSA[99] and CSA,[100] in respect of modification and control, under section 40A

---

92 Section 3.2.2.
93 Section 3.2.3.
94 Section 3.2.3.
95 Section 3.2.3.
96 Section 3.2.3.
97 Section 3.2.4.
98 Section 3.2.4.
99 Section 3.2.5.

(1)(*c*) of the NPA Act. SAPSA, CSA and NPA Act, also have similar provisions in respect of the contents of a computer. The penalty in terms of section 40A is a fine or imprisonment not exceeding 25 years or both, and much harsher than the ECT Act.[101] The CSA defines the term to, 'perform a function', whilst there appears to be no definition of in the NPA Act, bearing in mind the penalty clause. There does not appear to have been any reported cases imposing the maximum penalty.[102] Section 40A, together with the penalty clause will be deleted once the Cybercrimes Act 19 of 2020, is in operation.

In terms of section 66 of the Financial Intelligence Centre Act (FIC Act)[103] also refers to computers under their control. The maximum penalty is 15 years imprisonment or a fine not exceeding R10, 000.00. The FIC Act is closely related to the Prevention of Organised Crime Act[104] and the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.[105] The object of this Act was for the establishment of a Financial Intelligence Centre and a Money Laundering Advisory Council, imposing compliance on certain institutions and persons to combat money laundering.[106] The Cybercrimes Act will delete sections 65, 66 and 67, of the FIC Act once it is in operation.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act[107] referred to as RICA is to prohibit the intentional interception of communication. Section 4(1) provides the circumstances for the interception, and clearly not for the purposes of committing any crime. The criticism with RICA was the lack of transparency or adequate safeguards, as it has the most powerful mass surveillance capabilities that were not unregulated,[108] which findings were also made by the by the UN

---

100 Section 3.2.5.
101 Section 3.2.5.
102 Section 3.2.5.
103 Section 3.2.6.
104 Section 3.2.6.
105 Section 3.2.6.
106 Section 3.2.6.
107 Section 3.2.7.
108 Section 3.3.4.

Human Rights Committee.[109] On the 4 February 2021, in the judgment of *AmaBhungane Centre for Investigative Journalism*, the Constitutional Court ruled that RICA is unconstitutional in that it fails to provide appropriate provisions to protect the right to privacy regarding the freedom of expression; legal privilege; the independency of the designated Judge; notifying the subject of his or her surveillance; inadequate procedures and safeguards where the surveillance subject is a practising lawyer or journalist.[110] The unconstitutionality of these specific provisions may result in cyber offences that rely on data obtained pursuant to the interception of communications, adversely impacting on Extraditions. In the *AmaBhungane Centre for Investigative Journalism* case the majority judgment held that interception and surveillance of a person's communications is a highly intrusive privacy violation under RICA.[111]

There have been also criticisms with the Cybercrimes Bill of 2017, now the Cybercrimes Act 19 of 2020. Firstly, Chapter 2 of the Cybercrimes Act, has been criticized for seeking to regulate Malicious Communications, because it is open to abuse, especially with the definitions what messages are considered harmful.[112] The State Security Minister stated that regulations for social media's aim was to deal with fake or false news. The counter argument is that anything which is inherently false, under malicious communications will be a crime, and the concern is who decides what is false or not?[113] This will lead to Internet censorship and a suppression on freedom of expression.[114] This issue must be addressed in the Protection from Harassment Act,[115] and not additional criminal penalties imposed through the Cybercrimes Act.[116]

The R2K Campaign Also discussed the reforms to RICA, commenting firstly that the storage of a person's communication for up to five years[117] is unconstitutional. The second reform is the loophole of section 205 of the Criminal Procedure Act,[118] is a parallel procedure created to access people's

---

109 Section 3.3.4.
110 Section 3.2.7.
111 Section 3.2.7.
112 Section 3.3.1.
113 Section 3.3.1.
114 Section 3.3.1.
115 Section 3.3.3.
116 Section 3.3.3.
117 Section 3.3.3.
118 Section 3.3.4.

sensitive information outside the RICA judge's oversight.[119] The argument is that the Cybercrimes Bill, (now Cybercrimes Act) fails to take meaningful steps to correct the many loopholes in RICA, including the spy provisions, employing surveillance as a device for repression.[120]

Section 33 of the Cybercrimes Act does not allow an investigator or a citizen to effect an arrest, nor can the suspect be questioned for possession of suspected stolen goods. On further analysis of section 12 of the Cybercrimes Act, it includes theft of incorporeal property. Section 36 of the General Law Amendment Act[121] requires that police must request a person for an explanation, to give a satisfactory account of such possession, on a reasonable suspicion that goods have been stolen. An investigator, under the Cybercrimes Act would not be able to request a person for such an explanation, bearing in mind the right to privacy.

The purpose of the POPI Act is to protect the right to privacy, in terms of section 14 of the Constitution,[122] relating to the processing of personal information by data controllers and harmonise with international standards. Cookies and Cloud computing implies that there is no exclusive control over the personal data and the manner of data processing. The ECT Act fails to impose obligations on data controllers,[123] but POPI Act imposes obligations on information officers[124] which assists in preventing identity theft crimes.[125] POPI's origins come from European data protection law and the Organisation for Economic Co-operation and Development, (OECD), principles.[126] The EU's Directive,[127] imposed a strict prohibition on the transfer of personal data to non-member countries where there was not an adequate level of protection of the data processed. The General Data Protection Regulation (GDPR) replaced the Data Protection Directive because, of implementation challenges and the rapid development of technology. Part of the POPI Act was implemented on 1 July 2020, and with

---

119 Section 3.3.4.
120 Section 3.3.4.
121 Section 3.3.4.
122 Section 3.4.
123 Section 3.4.
124 Section 3.4.
125 Section 3.4.
126 Section 3.4.
127 Section 3.4.

effect from 1 July 2021, POPI is now fully implemented.[128] Professor A Roos did a comparison with selected provisions of both the GDPR and the POPI Act, to a ascertain whether amendments to the POPI Act are required to meet the minimum standards in respect of the EU Regulations on data protection. Roos found that the POPI Act should be amended to comply the GDPR, before approaching the EU for such a declaration of compliance.[129] Recommendations were made to amend the POPI Act, regarding consent.[130]

6.2.2.2 Finding

The Cybercrimes Act 19 of 2020, previously the Cybercrime Bill of 2017 removed the cybersecurity[131] bill. The Cybercrimes Act will be in full operation once proclaimed in the Government Gazette.[132] South Africa has a variety of cyber legislation that refers to unauthorised access to computers but limited to computers are under the direct control of that particular authority. The repeal of the sections in the various acts once the Cybercrimes Act comes into operation coalesces computer definitions.

The current cybersecurity legislation may not be apposite to satisfy the double criminality principle in respect of extraditable offences and extraditions will be onerous. The sophistication of technology consistently evolving, has drastically reshaped human life and modified the business world. South Africa lags at the back of superior economies in cybersecurity legislation.[133]

The lack the experience and skill in keeping up with superior economies delays implementation,[134] rendering legislation ineffective. There was never any Cyber Inspectorate or Cyber Inspectors that were appointed in terms of Chapter XII of the ECT Act to assist law enforcement, as well as the business and the public. In terms of the implementation regulations, these were not promulgated, and no offences were ever prosecuted.[135] Similarly this appears to be the case with no

---

128 Section 3.4.
129 Section 3.4.
130 Section 3.5.
131 Section 3.5.
132 Section 3.5.
133 Section 3.5.
134 Section 3.5.
135 Section 3.5.

prosecutions for cases of criminal defamation. Hopefully, the Cybercrimes Act will not be showcase legislation with slow or no implementation.

Law enforcement is to remind society that there can be no civilization without the rule of law, and an unpunished offender green lights like-minded people. Similarly, the extradition for cybercrime offences will be onerous in satisfying the double criminality if no offence exists in the requested state, or if the punishment was never enforced at the time of the request.[136]

There are many new cybercrime offences that now exist and the investigator[137] has wide powers of investigation, to search and seize[138] anything computer related. There must be the establishment of a designated Point of Contact[139] office within the South African Police Service (SAPS) for immediate assistance for investigations in respect of the commission of an offence.[140] The difficulty with this are the existing issues, amongst others; police budget cuts; the rise of crime; the breakdown and creation of specialized units; low morale; and community policing due to understaffed police service.[141]

The Cybercrimes Act relates only to cybercrimes and not cybersecurity. Violations of our cybersecurity could be perceived as a violation of our basic human right,[142] for failing to protect our data, our devices and the networks that are used. The protection of our personal information is critical and the POPI Act must be enforced.[143] POPI Act has been fully implemented since July 2021, which origin lies in the EU Directive. The EU Directive was repealed in 2018, and the POPI Act is substantially hinged on a law that is now repealed. A comparison of POPI to GDPR and the UK DPA may fall short on the international planes.[144]

---

136 Section 3.5.
137 Section 3.5; Cybercrimes and Cybersecurity Bill Republic of South Africa (published in *GG* 40487 of 9 December 2016) (hereinafter referred to the Cybercrimes Bill 2017), s 25.
138 Section 3.5; Cybercrimes Bill 2017, s 25 – definitions.
139 Section 3.5; Cybercrimes Bill 2017, s 52(1)(*a*).
140 Section 3.5; Cybercrimes Bill 2017, s 52(3)(*a*).
141 Section 3.5.
142 Section 3.3.4; Right2Know Campaign, 'R2K submission on the Cybercrimes Bill' (8 April 2017) <https://www.R2k.Org.Za/2017/08/11/R2k-Submission-on-the-Cybercrimes-Bill-2017> accessed 23 December 2020.
143 Section 3.3.4.
144 Section 3.5.

On the domestic plane, the further challenge is that part of the RICA Act has been declared unconstitutional, for the failure to provide apposite prophylactic measures to protect the right to privacy.[145] This may now easily afford opportunities for malefactors to openly and deliberately commit related POPI offences and theft without trepidation of prosecution or extradition.[146]

6.2.3 A compendium of the UK cyber laws, approach of the European Arrest Warrant and the United States cyber laws

6.2.3.1 Summary

The Computer Misuse Act 1990 (CMA), the Investigatory Powers Act 2016 (IPA), the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA), and the Network and Information Systems Regulation 2018 (NISR), the Fraud Act 2006 (FA), the Theft Act 1978, the Proceeds of Crime Act 2002 (POCA), Copyright, Designs and Patents Act 1988 are some of the cybersecurity laws in England and Wales.[147] The IPA, the Police Act of 1997 and the Intelligence Services Act, 1994 (ISA),[148] are utilised in cyber-attacks protecting the national and financial security. England, the US and South Africa are parties[149] to the Convention on Cybercrime.[150] The US is regarded as one of the predecessors for promulgating cybercrime laws in particular the Computer Fraud and Abuse Act[151] (CFAA).[152]

The UK-CMA, UK-IPA, UK-DPA, UK-NISR and UK-FA Acts are summarised. The UK Computer Misuse Act 1990 is considered to be the key cybersecurity regulations. Section 1 of UK CMA refers to unauthorised access and makes it an offence if the intent is to secure access to any program, and not any particular program or data.[153] The CMA creates three distinct criminal offenses namely; unauthorized access; the unauthorized access with intent to commit

---

145 Section 3.5; *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services*; *Minister of Police v AmaBhungane Centre for Investigative Journalism* NPC Case CCT278/19 & CCT279/19 [2021] ZACC [6]-[7].
146 Section 3.5.
147 Section 4.1.
148 Section 4.1.
149 Section 4.1.
150 Section 4.1.
151 Section 4.1.
152 Section 4.1.
153 Section 4.2.1.

further offenses, such as fraud or theft;[154] and the unauthorized modification of computer material. The criticism is that it is onerous to show that the person was aware that he or she was not authorised to access the service.[155]

- **The United Kingdom (UK)**

The Fraud Act 2006 and the Police and Justice Act 2006 were passed to tackle e-crime. The UK CMA was amended by the Police and Justice Act 2006 which introduced new offences regarding computer misuse together with increased penalties and amendments to the extradition legislation. In addition, the first e-crime guidelines, by the Association of Chief Police Officers (ACPO),[156] referred to as the ACPO Guidelines, was published to assist with outdated, inadequate practices and procedures. It is acknowledged as the best practise guidelines in digital evidence.[157]

The UK Investigatory Powers Act (IPA) provides a framework for the use of law enforcement agencies and investigatory powers to secure communications and data.[158] The Act also makes provision relating to the security, retention and examination of bulk personal datasets.[159] The Act extensively deals with various types of warrants for the lawful interceptions of communications. There are three kinds of warrants that may be issued in terms of section 15 of the UK IPA, namely,[160] the targeted interception warrants, targeted examination warrants, and mutual assistance warrants, with specific criteria for the use of the warrants. Section 99 refers to General Warrants;[161] targeted equipment interference warrants[162] and targeted examination warrants,[163] and again with specific criterion for the use of the warrants.[164]

The General Data Protection Regulation (GDPR), the Data Protection Act, 2018[165] (DPA), and the Network and Information Systems Regulation 2018

---

154 Section 4.2.1.
155 Section 4.2.1.
156 Section 4.2.1.
157 Section 4.2.1.
158 Section 4.2.2.
159 Section 4.2.2.
160 Section 4.2.2.
161 Section 4.2.2.
162 Section 4.2.2.
163 Section 4.2.2.
164 Section 4.2.2.
165 Section 4.2.3.

(NISR), impose obligations to protect personal data.[166] The origins to the DPA 2018, arose from the Convention for the Protection of Individuals with regard to automatic processing of personal data, referred to as Convention 108.[167] It is the first binding international instrument that contains a set of principles to prevent abuse of the collection and processing of personal data, and includes[168] the free movement of trans-border data with member states.[169] The DPA 2018,[170] supplements the EU General Data Protection Regulation (GDPR), which came into effect on 25 May 2018 and strictly regulates the collection, storage, and use of personal data. The old Convention 108,[171] was amended in accordance with the General Data Protection Regulation,[172] and is now called the modernized 'Convention 108+'.[173] This will allow states to share a powerful set of principles for the protection of personal data and provide a forum for cooperation on an international level.[174] The GDPR was enforced in the Google case. A historic precedent was set due to the failure to properly disclose to users the data collection across its services which resulted in the French data protection authority fining Google 50 million euros.[175]

The purpose of the UK Network and Information Systems Regulation 2018 (NISR) Act[176] comes from the NIS Directive, to ensure that essential services have sufficient measures for the security of their network and information systems. Its aim is to avert harm and risk to the UK's economy and society, to ensure that the UK is secure and resilient to cyber threats, robust and sanguine in the digital world.[177] Member States were required to bring the Directive into their domestic legislation.[178] The National Cyber-Security Centre (NCSC), was established to have a Single Point of Contact[179] and a Computer Security

166 Section 4.2.3.
167 Section 4.2.3.
168 Section 4.2.3.
169 Section 4.2.3.
170 Section 4.2.3.
171 Section 4.2.3.
172 Section 4.2.3.
173 Section 4.2.3.
174 Section 4.2.3.
175 Section 4.2.3.
176 Section 4.2.4.
177 Section 4.2.4.
178 Section 4.2.4.
179 Section 4.2.4.

Incident Response Team[180] to undertake its responsibilities under the Intelligence Services Act.[181]

The UK Fraud Act 2006 provides that fraud may be committed in three ways; by false representation,[182] by failing to disclose information[183] and by abuse of position.[184] It creates new offences including obtaining services dishonestly,[185] possessing and making or supplying articles for use in frauds,[186] and to adapt, supply or offer to supply any article in connection with fraud, for example the electricity meters or its malfunction. It is interesting to note that meaning of 'article' is broadened to include any program or data held in electronic form.[187]

The UK recognised that it may be difficult with the many laws including the cyber and cybersecurity laws, to deal with extraditions between states, and to satisfy the double criminality principle. The introduction of the European Arrest Warrant (EAW),[188] in 2002, was to make procedures expeditious, simple, and unified,[189] deviating from the from traditional extradition procedures. The European Arrest Warrant was a Framework Decision[190] based on the top-echelon of confidence between the Member States. It abolishes extradition and the requirement of double criminality for certain offences and replacing it with a system of surrender between judicial authorities. The phrases 'extradition' is replaced with the phrase 'surrender', and the terms 'applicant State' and 'soliciting' state are replaced with 'issuing judicial authority and enforcement' or 'the issuing State and the executing Member State'.[191] The court pronounced on the validity of the European Arrest Warrant and the Framework Decision and found no contravention on both the principles of legality in criminal proceedings or equality. The decisions regarding the execution of the European arrest warrant must be subject to sufficient controls and judicial authority, whilst the central authority's role be limited to practical and administrative assistance.

---

180 Section 4.2.4.
181 Section 4.2.4.
182 Section 4.2.5.
183 Section 4.2.5.
184 Section 4.2.5.
185 Section 4.2.5.
186 Section 4.2.5.
187 Section 4.2.5.
188 Section 4.1.
189 Section 4.1.
190 Section 4.3.
191 Section 4.5.

There is also provision for mandatory non-execution of the EAW and optional non-execution for a citizen or resident. What is important is that judicial oversight is obligatory.[192] Since Brexit, with the UK's departure from the EU, both the UK and EU concluded the Trade and Cooperation Agreement.[193] The European Arrest Warrant no longer applies to the UK, but still applies to persons arrested under an European Arrest Warrant prior to the agreement.[194]

- **The United States (US)**

Cybercrime law in the United States is summarised in respect of the Computer Fraud and Abuse Act (CFAA) of 1984, the Economic Espionage Act of 1996 and the National Information Infrastructure Protection Act of 1996 (NIIPA). The US CFAA introduced three new federal crimes on the access of a computer without authorisation, specifying the circumstances. The crimes relating to government are computer misuse to obtain national security secrets, personal financial records, and hacking into government computers.[195] The CFAA was enacted in 1986 as Congress intended to prevent unauthorized access relating to 'federal interest' and provided additional penalties. The statute was intended to criminalise only important federal interest computer crimes,[196] but now has the effect of potentially regulating every computer in the U.S and millions of computers overseas.[197] Congress extended the CFAA to further protect computers and networks from accidental damage, even without any negligence. The scope and coverage of the CFAA was continuously broadened through subsequent amendments.[198]

In the interesting case of *United States of America v Vladimir Tsastsin and 6 Others*,[199] the defendants and their co-conspirators ran companies that did subterfuge as legitimate in the Internet advertising industry and the defendants faced charges of 'click hijacking fraud' and 'advertising replacement fraud'.

---

192 Section 4.5.
193 Section 4.3.
194 Section 4.3.
195 Section 4.4.1.
196 Section 4.4.1.
197 Section 4.4.1.
198 Section 4.4.1.
199 Section 4.4.6.

The US Economic Espionage Act of 1996[200] was expanded in three different ways by[201] expanding the term unauthorised access; adding new provisions to the computer damage prohibition; and adding a computer extortion statute. The significant change was that 'federal interest' computers were replaced with the new category of 'protected computers'.[202] The National Association of Criminal Defence Lawyers (NACDL) points out that the word 'used' in interstate commerce is broad, and every computer that is connected to the Internet is used in interstate commerce and falls into the interpretation of a 'protected computer' covered by 18 U.S.C. § 1030, which may result in over criminalisation.[203]

The US National Information Infrastructure Protection Act of 1996 (NIIPA) expanded subsection (*a*)(2)[204] firstly; by stating that information is protected, only if an interstate or a foreign component is involved in this conduct.[205] Secondly; computer extortion is penalised, and[206] thirdly; by expanding the list of damage.[207] The definition of 'protected computer' was again expanded by the USA Patriot Act.

The USA Patriot Act was passed by Congress after World Trade Centre was attacked on September 11, 2001.[208] The crucial change was the definition of 'protected computer' was expanded to include computers located outside the United States which harms interstate or foreign commerce or communications. The Patriot Act, was replaced with the USA Freedom Act (H.R. 2048), in 2015, restricting the government's authority to collect data and banning the bulk collection of the private records which was under section 215 of the USA Patriot Act.[209]

---

200 Section 4.4.2.
201 Section 4.4.2.
202 Section 4.4.2.
203 Section 4.4.2.
204 Section 4.4.2.1.
205 Section 4.4.2.1.
206 Section 4.4.2.1.
207 Section 4.4.2.1.
208 Section 4.4.3.
209 Section 4.4.3.

6.2.3.2 Finding

Section 1 of the UK Computer Misuse Act 1990,[210] criminalises the causing of a computer for unauthorised access while operating on the Internet. Section 2 also criminalises the intentional unauthorised access and activities for impairing computers.[211]

The UK Investigatory Powers Act provides a framework that sets out the criteria to be met before exercising sensitive and intrusive powers which requires Judicial Commissioners to approve the issuing of warrants. The Investigatory Powers Act is a critical piece of legislation which will help to facilitate the creation of improvement of South African cybersecurity law.[212] The referral to different types of warrants specifying the grounds and details for the warrant will result in less (fewer) infringements of a person's right to privacy and protection of personal information.

The UK Data Protection Act 2018 complements the General Data Protection Regulation, regulating the processing of data by various competent authorities. Provision is made for Information Commissioner to effect enforcement of the data protection legislation.[213]

The UK European Arrest Warrant has proved itself to be the most illustrious in the history of extradition, especially in terms of simple and speedy procedures.[214] The requirement of double criminality for certain offences is abolished and is replaced with a structure of 'surrender' between judicial authorities.

The US Computer Fraud and Abuse Act (CFAA)is one of the most extensive and wide-ranging criminal laws in the federal code,[215] due to the continuous expansion over the years through congressional amendments. Kerr argues that courts are to adopt narrow interpretations in light of the void-for-vagueness

---

210 Section 4.5.
211 Section 4.5.
212 Section 4.2.2.
213 Section 4.5.
214 Section 4.5.
215 Section 4.5.

doctrine. The CFAA has become too broad and the meaning of unauthorised access is notably unclear.[216]

The ECT Act does not specifically deal with offences like those contained in the US indictment of cyber fraud. The US CFAA, and the US Indictment[217] has offences of; click hijacking, Advertising Replacement Fraud,[218] Conspiracy to commit computer intrusion,[219] Wire Fraud charge, Computer Intrusion Furthering Fraud and Computer Intrusion by Transmitting data. South Africa's Cybercrimes Act[220] creates new cybercrime transgression,[221] but can these new offences compare to the US CFAA, especially in respect of an extradition request that covers the double criminality in respect of the US CFAA and Wire Fraud Statute and the issue of specialty.

6.2.4 The rule of law, aut dedere aut judicare (extradite or trial), and mutual legal assistance

6.2.4.1 Summary

The rule of law's axiom is that all persons are bound by the laws of the state, and which are enforced by the courts.[222] Domestic legislation was passed implementing the Rome Statute of the International Criminal Court, and South[223] Africa bound itself to international obligations. The *aut dedere aut judicare* principle means that the state must effect an extradition, save for the certain exceptions, or establish jurisdiction, in which case the state must then punish an offender under its own laws.[224] Article 6 of the European Convention on Extradition confers the right to refuse extradition of a state's own nationals. The rationale for the refusal is the be the fear that their nationals will not receive a fair trial or fitting punishment. In the case of Mr Henry Emomotimi Okah,[225] a Nigerian national with permanent residency in South Africa, was charged with 13 counts relating to terrorism under the Protection of Constitutional Democracy

---

216 Section 4.5.
217 Section 4.4.6.
218 Section 4.4.6.
219 Section 4.4.6.
220 Section 3.5.
221 Section 3.5.
222 Section 5.1.
223 Section 5.1.
224 Section 5.1.
225 Section 5.3.1.

against Terrorist and Related Activities Act.[226] The Accused was not extradited but prosecuted in the Johannesburg High Court. On appeal, the issue of jurisdiction was settled when the Constitutional Court declared that South African courts have extra-territorial jurisdiction in terms of section 15(1) of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, rejecting the SCA's approach as narrow and with inanities.[227] South Africa is a part of the international community in the scrimmage against terrorism.[228]

In terms of section 18 of the Criminal Procedure Act[229] the State, save for certain offences, may not institute criminal proceedings if twenty (20) years have passed from the date that of the offence. The Extradition Treaty between the Republic of South Africa and the Argentine Republic refers to an extradition is requested that would be barred by prescription under the law of the requesting State but does not refer to the requested State. The situation that may arise is that an offence that has prescribed in South Africa would render a surrender contrary to the double criminality principle.[230]

The European Convention on Mutual Assistance in Criminal Matters acknowledges that mutual legal assistance is closely related linked to extradition, and vital for investigations. Mutual legal assistance (MLA) must be swift for cybercrime to be efficacious due to the transnational and capricious nature of electronic evidence.[231] South Africa's struggle regarding digital evidence investigations and prosecutions[232] could be present a challenge in extraditions or mutual legal assistance for cybersecurity offences, both locally and globally. The maxim of *nulla poena sine lege*, is enshrined in the supremacy constitution of the Republic of South Africa which is based on sovereignty, democracy and the rule of law.[233]

There is no crime without a law, which comes from the maxim: *nulla poena sine lege*.[234] An extradition would not be lawful in the absence of the correct

---

226 Section 5.3.1.
227 Section 5.3.2.
228 Section 5.3.2.
229 Section 5.2.4.
230 Section 5.2.4.
231 Section 5.1.
232 Section 5.2.1.
233 Section 5.2.1.
234 Section 5.2.1.

procedures being followed. The rule of law must apply to all persons, and a disregard for the rule of law was seen in the cases of; former head of Rwandan intelligence, Kayumba Nyamwasa, where South Africa granted him refugee status, in-spite of various extradition requests;[235] and in the case of Guus Kouwenhoven, a Dutch war criminal was requested by Netherlands to serve his 19-year sentence but was still issued with a South African visa.[236]

An assessment was done by the Cybercrime Convention Committee (T-CY), on the efficiency of mutual legal assistance and Article 31 of the Budapest Convention on Cybercrime relating to stored computer data for international coopetition. The Budapest Convention's aim is for states to have harmonisation in cybercrime laws, but no African country has ratified this treaty.[237] The Committee made several findings, namely; mutual assistance for obtaining stored computer data was not only related to computer offences, but also Fraud and other financial crimes; due to the convoluted nature of electronic evidence in MLA, investigations are often ditched; spontaneous information is underutilized; minor cases are burdensome, and MLA requires dual criminality in respect of requests for stored computer data.[238]

The committee also found, amongst others, several problems relating to a MLA request, namely; time, caseload difficulty; length of time in responding to a request; no cooperation; the dual criminality requirement becomes problematic; and limited high-tech skills.[239] The Parties to the Budapest Convention on Cybercrime, the European Convention on Cooperation in Criminal Matters treaty,[240] and the 2nd Additional to the treaty (ETS 182), allows for direct coopetition between judicial systems.[241] South Africa is only a signatory, and a request will probably fall into the problems that is experienced, with urgency being lost.[242]

Transborder efficacy becomes vital in cyber offences, due to no online crime scene in cyberspace. Jurisdiction is based on the principle of territoriality and

---

235 Section 5.2.1.
236 Section 5.2.1.
237 Section 5.4.1.
238 Section 5.4.1.
239 Section 5.4.1.
240 Section 5.4.1.
241 Section 5.4.1.
242 Section 5.4.1.

the difficulty is the place of origin of cybercrime. Article 32[243] of the Budapest Convention on Cybercrime has been criticized[244] for; not covering Transborder searches as they may be a breach of sovereignty; article 32(*b*) applies only by consent of the individual; article 32 is regarded as a controversial provision.[245]

The many concerns and safeguards would have to be looked into regarding the powers for transborder access to data and jurisdiction, and the Budapest Convention does not allow blanket transborder access.[246] In the case of '*Correctionele Rechtbank van Antwerpen, afdeling Mechelen*' of Belgium, the judge of Mechelen ordered wiretapping of a suspect's Skype account in Luxembourg. The court said that the accused was a voluntarily service provider in the Belgian market, and the court confirmed jurisdiction.[247]

6.2.4.2 Finding

The Budapest Convention on Cybercrime[248] is a multilateral agreement that addresses the cybercrime with confluent acts of codification.[249] Countries, including South Africa are encouraged to become signatories to the Cybercrime Convention, in order to acquire and secure technical assistance[250] for effective transborder access to data and jurisdiction.[251]

Some of the findings of the Cybercrime Convention Committee (T-CY),[252] regarding MLA are complexity, prolonged due to obtaining electronic evidence, and often is not pursued.

The Cybercrimes Act creates new cybercrime offences, however there are several criticisms that were raised in the Bill. Extraditions or prosecutions relating to cybersecurity offences may be difficult,[253] due to the Cybercrimes Act making no reference to the Cybersecurity Bill.

---

243 Section 5.4.2.
244 Section 5.4.2.
245 Section 5.4.2.
246 Section 5.4.3.
247 Section 5.4.3.
248 Section 5.5.
249 Section 5.5.
250 Section 5.5.
251 Section 5.5.
252 Section 5.5.
253 Section 5.5.

The essence of the *aut dedere aut judicare* principle is a refusal to extradite one's own national, but the State must proceed with a prosecution. South Africa has an obligation to prosecute or extradite. It has been proposed that in the event of the territorial state proceeding with trial, then there should be expatriation to the home state for sentence and rehabilitation.[254]

Jurisdiction traditionally limited within a state's territory has been relaxed by international terrorism conventions.[255] South African jurisprudence confirms extra-territorial jurisdiction in terms of section 15 of Protection of Constitutional Democracy against Terrorist and Related Activities Act. South Africa has an obligation to combat terrorism and to bring to trial malefactors of terrorism, wherever perpetrated and anyone that it does not extradite,[256] as in the Okah case.

There can be no prosecutions in the absence of legislation, and the cyber-security Bill is not part of the Cybercrimes Act.[257] The National Cybersecurity Policy Framework (NCPF),[258] of 2015, has been prolonged and its uncertain when it will be passed. The inadequacy of security legislation has the repercussion of fearlessness for the law or extraditions.[259] This is evident from the case of Experian data breach of twenty-four million South Africans and eight hundred thousand businesses, which to date has had no ramifications. The further problem was that a Russian attacker was implicated and the president made a statement that Russia does not extradite its nationals.[260] The Cybercrimes Act is not fully in operation, and possibly with no retrospective operation, so the offence of theft of incorporeal property may never be prosecuted. Experian took the point that the data breach was innocuous.[261]

UKs Network and Information Systems Regulations (NISR)[262] legislation, ensures that appropriate measures are in place for the security of their network and information systems. Statistics reveal SA to be among the countries with

---

254 Section 5.5.
255 Section 5.5.
256 Section 5.5.
257 Section 5.2.2.
258 Section 5.2.2.
259 Section 3.5.
260 Section 5.2.2.
261 Section 5.2.2.
262 Section 5.2.2.

the highest number of cybercrime victims, malware attacks, legislation akin to NISR should exist in South Africa. Cyber malefactors are targeting both the South African public and the private sector in well organised attacks, and the question is why? The coronavirus pandemic provided fortuitousness on impersonation fraud, which saw an increase of 75% of attacks in the first 100 days.[263]

In the *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services*, the court found that parts of RICA were inconsistent with the Constitution, in that there was a no legal basis for the state to conduct bulk surveillance. The practice of bulk interception was unlawful and baseless.[264]

South Africa has assented on the 6 November 1996 to the International Co-Operation in Criminal Matters[265] (ICCM) in respect of mutual legal assistance.[266] Section 2(2)[267] is considered onerous, too inflexible, and could result in an application being unsuccessful. The Namibian International Co-operation in Criminal Matters Act approach is to be followed. Whilst provision is made for reciprocal assistance in the execution of orders in criminal matters, no provision exist for the implementation of foreign prison sentences in South Africa.[268]

6.3 Recommendations

6.3.1 Legislation and treaties

6.3.1.1 Legislation

- The criticism of the Cybercrimes Act,[269] relates to section 33(1) regarding searching, accessing to, or seizing of an article on arrest of a person. This must be amended to include a citizen's arrest, which is a provision allowed in terms of section 42 of the Criminal Procedure Act.[270] This will allow an investigator or a private person to effect a citizen's arrest. The capacity to

263 Section 5.2.2.
264 Section 5.2.3.
265 Section 5.5.
266 Section 5.5.
267 Section 5.5.
268 Section 5.5.
269 Section 3.3.4.
270 Section 3.3.

fight genuine cybercrime and make cyberspace[271] more secure is not going to succeed if it's left solely in the hands of the police. The securing of digital evidence is vital in cybercrimes, provided the data extracted from the computer system most importantly satisfies the requirement of admissibility.[272] The amendment will allow an investigator or a private person to efficaciously secure and preserve evidence, for prosecutions, extraditions and mutual legal assistance.

- Cyber security for government agencies is to ensure the state knows what's happening on the Internet and can intervene when someone does something wrong.[273] The inadequate cybersecurity law currently in South Africa provides criminals with the opportunity to commit cybercrimes, without the fear of a prosecution or extradition,[274] as in the Experian data breach case example.[275] The Cybercrimes Act should be amended, to allow the law enforcement agencies to shut down websites that are not in terms of the Financial Intelligence Centre Act 2001,[276] compliant with South African law, after notice has been given to them and they have failed to comply.

- Our law is settled that the double criminality principle, in respect of a criminal offence, applies from the date of the extradition request,[277] which is a departure from the United Kingdom.[278] The recommendation is that section 18 of the CPA[279] has to be amended. This section refers to domestic law to the time the offence was committed but is silent on the point of extraditions. Section 18 of the Criminal Procedure Act of 1977[280] determines that the State may not institute criminal proceedings against a suspect if 20 years have passed from the date that the offence was committed. Section 18 be amended to read:

---

271 Section 3.3.
272 Section 4.2.1.
273 Section 3.3.4.
274 Section 3.5.
275 Section 5.2.2.
276 Section 3.2.6.
277 Section 2.3.1.3.
278 Section 2.3.1.1.
279 Section 5.2.4.
280 Section 5.2.4; Act 51 of 1977.

18 Prescription of right to institute prosecution

The right to institute a prosecution for any offence, other than the offences, (specified in the section), shall, unless some other period is expressly provided for by law, *or where a person is a fugitive from justice* (the amendment), lapse after the expiration of a period of 20 years from the time when the offence was committed.

- In 2003 South Africa acceded to the European Convention on Extradition of 1957[281] and its Additional Protocols. It is recommended that there is no reason for South Africa not to become a member of the European Union for the purposes of harmonisation of extradition procedures. The European Union with the introduction of the Schengen agreement has positively impacted on transnational crime in terms of expeditiousness.[282] This has influenced and motivated innovative techniques for the surrender of offenders with Member States, constructed on uniformity and easy procedures replacing the traditional extradition approach.[283] The European arrest warrant[284] is identical to that of extradition,[285] but abolishes extradition and the requirement of double criminality for certain offences.[286] 'The national executing judicial authorities and the courts, recognises the request of the issuing judicial authority of another Member State on handing over persons after checks and conditions for issuing the mandate'.[287] The importance is Judicial oversight, for the surrender of a person, and exemption from the rule of dual criminality regardless of the name in the issuing state's law,[288] which is beneficial if South Africa wants

---

281 Section 2.2.2.

282 Section 4.3. Eleni Cristina Marcu, 'The Execution of the European Arrest Warrant' (2016) 65 The Juridical Current 132-139.

283 Section 4.3; Marcu, 'The Execution of the European Arrest Warrant' 132-139.

284 Section 4.3.

285 Section 4.3. Council of the European Union, 'Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States (13 Jun 2002)' (2014) 1 International Law & World Order 1.

286 Section 4.3.

287 Section 4.3; see LAW - no 377 of 31 May 2011 Law no 302/2004, republished in the Official Gazette of Romania, Part I, 'Law302republished_amended_en' accessed 12 May 2020.

288 Section 4.3; see LAW - no 377 of 31 May 2011 Law no 302/2004, republished in the Official Gazette of Romania, Part I, 'Law302republished_amended_en' accessed 12 May 2020.
In Article 96 Law no 302/2004 are mentioned distinct categories of offenses for which a European arrest warrant can be enforced by the Romanian judicial authorities, as they were taken from the decision and are exempt from the rule of dual criminality regardless of the name, they have in the issuing state law.

to try to tighten and close the gap with cybercrime offences and extradition.

6.3.1.2 Treaties

- South Africa has already acceded to the European Convention on Extradition of 1957,[289] and should ratify all the protocols; 185,[290] 182[291] and No 30.[292] SA is a signatory[293] to the Convention on Cybercrime Number 185, which was signed on the 23/11/2001, but has never ratified it. The Cybercrimes Convention 185 should be ratified as we now have in place our Cybercrimes Act 19 of 2020. The Cybercrimes Convention acknowledges that the consequences of criminal behaviour are not geographically bound,[294] and the repercussions of the criminal act are far away from the crime scene.[295] These problems must be solved by international law, with adequate measures.[296] The aim is to deal with both, substantive and procedural issues together with international criminal law procedures and protocols.[297] The Convention focuses on; harmonising the domestic criminal substantive law elements of offences in the area of cybercrime; providing for domestic criminal procedural law powers for the investigation and prosecution of offences including those committed by means of a computer system or in the electronic form; and setting up a fast and effective regime of international co-operation.[298]

- The Convention already addressed the concerns[299] regarding the cyber-space offences of telecommunication networks, including the Internet's illegal money transactions, illegal services, and those which violate human dignity; uniformity with the objective of international partnership including sanctions**;** the possibility of transborder use, with examples of interception,

---

289 Section 2.2.2.
290 Section 4.1.
291 Section 5.4.1.
292 Section 5.4.1.
293 Section 5.4.1; Council of Europe, 'List of Treaties' (1 May 2012) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/209?module=signatures-by-treaty&treaty num=185> accessed 12 May 2020.
294 Section 5.4.1; T-CY Explanatory Report 1.
295 Section 5.4.1; T-CY Explanatory Report 2.
296 Section 5.4.1; T-CY Explanatory Report 2.
297 Section 5.4.1; T-CY Explanatory Report para 10 on 2.
298 Section 5.4.1; T-CY Explanatory Report para 16 on 4.
299 Section 5.4.1; T-CY Explanatory Report para 11 on 3.

surveillance of networks via the Internet, search and seizures in data-processing systems and websites**;** the issue of jurisdiction of the location (*locus delicti*) and the applicable law, including the problem of *ne bis idem* dealing with multiple jurisdictions and solving jurisdiction conflicts**;** investigation of cyber-space offences, and working closely with the Committee experts on the Operation of European Conventions in the Penal Field (PC-OC).[300]

- The European Convention on Mutual Assistance in Criminal Matters, 30, states that mutual assistance is related to the question of extradition, which is the subject of the Convention signed on 13th December 1957, and South Africa is not a signatory.[301]

  The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters 182 signed in Strasbourg, 8 November 2001, aimed to improve States' ability to react to cross-border crime and in light of technological developments throughout the world. It supplements the 1959 Convention and the 1978 Additional Protocol to it, by broadening the circumstances of which mutual assistance, making provision for assistance easier, quicker and more flexible. It also acknowledges the need to protect individual rights in the processing of personal data.[302]

6.3.2 Recommendations on mutual legal assistance

The Cybercrime Convention Committee (T-CY),[303] assessed the efficiency of the international cooperation provisions in the Budapest Cybercrime Convention. The committee recognised that expeditiousness is essential for efficacy in electronic offences, considering international relations and the vaporous type of data.[304]

Recommendation 1: There should full implementation of the provisions of the Convention, including preservation measures.[305]

---

300 Section 5.4.1; T-CY Explanatory Report para 11 on 3.
301 Section 5.4.1; Council of Europe, 'List of Treaties'.
302 Section 5.4.1; Council of Europe, 'List of Treaties'.
303 Section 5.1.
304 Section 5.1.
305 Section 5.1.

Recommendation 2: Parties keep statistics for monitoring the efficiency of the process regarding cybercrime and computer evidence.[306]

Recommendation 3: There must be adequate technology-literate staff at the prosecution authority for the execution of requests.[307]

Recommendation 4: Provision must be made for better training and there should be direct police-to-police communication. Expertise sharing with prosecution and judiciary is important, encouraging direct cooperation between judicial authorities and supported by skills development programmes of the Council of Europe and other organisations.[308]

Recommendation 5: Work towards strengthening the role of 24/7 points of contact in line with article 35 Budapest Convention, including:[309]

a. Skilled personnel to assist in the operations and support structures;

b. Contact points to be proactive in advocating their importance with domestic and foreign offices;

c. Conduct conferences and keep abreast with skills development of the 24/7 network with domestic and foreign authorities;

d. Encourage the appraisal of procedures of the 24/7 points of contact and provide feedback to the requesting State on Article 31 requests;

e. Consider establishing contact points within the prosecution authority for more direct involvement and speedier responses relating to requests.

Recommendation 6: Streamline the process, shorten procedures for requests and share best practices.[310]

Recommendation 7: Make use of all available channels for international cooperation.[311]

---

306 Section 5.1.
307 Section 5.1.
308 Section 5.1.
309 Section 5.1.
310 Section 5.1.
311 Section 5.1.

Recommendation 8: There must be emergency measures to deal with situations that are exigent and lethal.[312]

Recommendation 9: There must be acknowledgement of the requests received with notification of the measures taken.[313]

Recommendation 10: Broaden the domestic investigation scope when a foreign request or when information is received for facilitating and sharing information.[314]

Recommendation 11: Use of electronic transmissions for a request in alignment with article 25.3 with the Budapest convention to expedite communication mechanism.[315]

Recommendation 12: Parties must make sure that requests are specified with supporting information.[316]

Recommendation 13: The application of dual criminality must be flexible to facilitate the request for assistance.[317]

Recommendation 14: Consultations with the requesting authorities prior to the requests.[318]

Recommendation 15: There must be transparency in the process, reasons for refusing a request, central authorities to stipulate requirements and thresholds on websites.[319]

6.3.3 Recommendations[320] by the committee for an additional protocol to the Budapest Convention on Cybercrime

Recommendation 19: Allows for the disclosure of information relating to a specific IP address or user account.

---

312 Section 5.1.
313 Section 5.1.
314 Section 5.1.
315 Section 5.1.
316 Section 5.1.
317 Section 5.1.
318 Section 5.1.
319 Section 5.1.
320 Section 5.1; see para 5.2.4 T-CY Explanatory Report 127.

Recommendation 20: Prospects and extent for direct cooperation with both authorities for issuing of an international order.

Recommendation 21: Enhance immediate coopetition with judicial officials.

Recommendation 22: Address the implementation and enforcement processes, for the direct obtaining data from foreign service providers with safeguards.

Recommendation 23: Teamwork and concerted efforts in investigations.

Recommendation 24: The use of English language be permitted.

6.3.4 Recommendations on cybersecurity

6.3.4.1 The Tallinn manuals

The 2015 draft version of the Cybercrimes and Cybersecurity Bill was rejected in its entirety, with having deep fundamental flaws, threatening the democratic spirit of the Internet.[321] The Cybercrimes Act has removed all reference to the draft cybersecurity legislation. Although with the creation of this Cybercrimes Bill, South Africa attempted to strengthen its international relations in terms of cooperation,[322] it cannot do so in isolation with the implementing of the Cybercrimes Act only. South Africa is still developing legislation and policy regarding cybersecurity activities bearing in mind the pace of technology and the procedural elements of law making are time consuming.[323] The felicitousness of the Tallinn Manuals[324] would be a foundation of best practice to enhance the current legislation.[325]

Technology has fundamentally outgrown laws, governance processes and cybercrime has escalated the need for the development of legal frameworks.[326] Cyber-operations that breach international law will at some point become the norm, however, the current absence of a legal framework poses a major challenge,[327] in cybersecurity. The Tallinn Manuals were produced by an

---

321 Section 4.2.2.
322 Section 4.2.1.
323 Section 4.2.1.
324 Section 4.2.1.
325 Section 4.2.1.
326 Section 4.2.1.
327 Section 4.2.1.

international group of experts and participants[328] for this purpose but still require international cooperation[329] and persuasion. South Africa would benefit from such international cooperation in terms of the law on cyber operations.[330] South Africa should use the Tallin Manuals as a guide for rules governing cyber operations which provides extensive commentary on each rule. The Tallinn Manual 2.0 expands its coverage of the international law governing cyber warfare to peacetime legal regimes, addressing topics of sovereignty, State responsibility, human rights, the law of air, space, and the sea.[331]

6.3.4.2 The Association of Chief Police Officers (APCO)[332] guidelines

The supremacy of the Constitution gives direction on implementation not only to the South African police services (SAPS) but to all laws, structures and all public organisations.[333] The police must meet expectations of compliance with laws, guidelines and systems but also adapt to technological change.[334] The ACPO[335] guidelines was the first e-crime guidelines to be published,[336] and acknowledged as the best practise guidelines ever produced to abet law enforcement in handling digital evidence.[337] The recommendation should be considered that South Africa develops an extensive, pliant and appropriate policing model by integrating some of the worldwide good policing practices,[338] including the APCO guidelines. The Cybercrimes Act[339] gives the police immense powers in respect of investigations, searches and seizures, and may lead to abuse or misuse of powers due to lack of expertise.

The R2K Campaign stated that ‘what the Cybercrimes Act doesn’t do and can’t do, is develop the expertise within the police force, detect and solve

328 Section 4.2.1.
329 Section 4.2.1.
330 Section 4.2.1.
331 Section 4.2.1.
332 Section 4.2.1.
333 Section 4.2.1.
334 Section 4.2.1.
335 Section 4.2.1.
336 Section 4.2.1.
337 Section 4.2.1.
338 Section 4.2.1.
339 Section 3.3.

cybercrimes and the expertise inside the State to create better defences against cybercrime'.[340]

6.3.4.3 The UK Investigatory Powers Act (IPA)[341] of 2016

South Africa could benefit from the UK IPA to provide a good guideline with cybersecurity. Extraditions may prove to be a challenge regarding the specialty of crimes, in the absence of adequate cybersecurity legislation for offences referred to in the UK IPA Act.[342]

The IPA provides a useful framework for law enforcement agencies and the investigatory powers to secure communications and data.[343] The Act also makes provision relating to the security, retention and examination of bulk personal datasets.[344] The Act extensively deals with various types of warrants for the lawful interceptions of communications. There are three kinds of warrants that may be issued in terms of section 15 of the IPA, namely,[345] the targeted interception warrants, targeted examination warrants, and mutual assistance warrants, with specific criteria for the use of the warrants. Section 99 refers to General Warrants;[346] targeted equipment interference warrants[347] and targeted examination warrants,[348] and again with specific criterion for the use of the warrants.[349]

6.3.4.4 Recommendations by Professor Roos on the POPI Act[350]

- It should be requirement that there be an affirmative clear consent. Consent must be explicit for processing of special categories of personal information.
- The processing of personal information is necessary if it is in terms of a legal obligation. The processing of personal information for the protecting of the interests of the data subject should be vital. The processing of

---

340 Section 3.3.3.
341 Section 4.2.2.
342 Section 4.2.2.
343 Section 4.2.2.
344 Section 4.2.2.
345 Section 4.2.2.
346 Section 4.2.2.
347 Section 4.2.2.
348 Section 4.2.2.
349 Section 4.2.2.
350 Section 3.5.

personal information to fulfil the obligations of the data controller in the field employment or any other particular field should be lawful, or by agreement or by contract.

- The GDPR states that only an official authority may keep a comprehensive register of criminal convictions. The processing of personal information of the data subject, on the basis of the public interest, should be substantial with suitable and specific measures safeguarding fundamental rights and the interests.
- The further recommendation by Roos is that provisions relating to the procedural and enforcement mechanisms, the data-protection principles and data subject rights be evaluated to ascertain whether the POPI Act meets the international standard of the GDPR.[351]

6.3.4.5 Recommendations on US cyber offence prosecutions

South Africa's ECT Act,[352] refers to offences relating to; Unauthorised access, interception of or interference with data, (e.g., so-called 'hacking') and computer related extortion, fraud and forgery.[353] The ECT Act does not specifically deal with offences like that contained in the US indictment. The Us indictment should be used as a precedent and guide for drafting of charges or indictments. It also should guide our jurisprudence in expanding the common law scope of Fraud.

The indictment[354] in the matter of *United States of America versus Vladimir Tsastsin and 6 others* is formidable to see that common law fraud has evolved to a whole new dimension in relation to cybercrime fraud. This indictment sets out many charges, with the first count being conspiracy to commit wire fraud.[355] South Africa does not have a similar provision for such an offence.

---

351 Section 3.5.
352 Section 3.2.2.
353 Section 3.2.2.
354 Section 4.4.4. United States District Court, Southern District of New York, Sealed Indictment 82-11 Cr-878 *United States of America v Vladimir Tsastsin*, Andrey Taamei, Timur Gbrassimenko, Dmitri Jegorov, Valerri Aleksejev, Konstantin Poltev and Anton Ivanov <https://www.justice.gov/usao-sdny/programs/victim-witness-services/united-states-v-vladimir-tsastsin-et-al-11-cr-878> accessed 15 May 2021.
355 Section 4.4.4.

In contrast to South Africa and looking at the ECT Act, no Cyber Inspectors were appointed, and no transgressions created by Chapter XIII were ever prosecuted.[356]

The indictment describes the conduct where the defendants and their co-conspirators operated and controlled companies that masqueraded as legitimate participants in the Internet advertising industry, and devising a sophisticated scheme by infecting malware in millions of computers that surreptitiously caused those infected computers to be redirected to websites that generated illicit advertising revenue.[357] It is interesting to see that the components of this advertising fraud scheme included what this Indictment refers to as (i) 'click hijacking fraud' and (ii) 'advertising replacement fraud'. South Africa is still yet to deal with these specific types of offences. The common law fraud with the element of misrepresentation would still apply in South Africa, together with the Cybercrimes Act, once it is in operation. The indictment referred to examples of how the click hijacking fraud worked and included the following: a) The Apple iTunes example,[358] where the link for the official Apple-iTunes website was instead redirected to a different site. b) The Netflix example refers to how the user was redirected to an unrelated website. c) The Internal Revenue Service example refers to how the user clicked on a link and redirected another to the website.[359]

The indictment referred to the Advertising Replacement Fraud,[360] which was another component of the defendant's fraud scheme, involving the replacement of legal advertisements on websites for monetary gain. The examples included the Wall Street Journal, Amazon.com and the ESPN website, where the Defendants reaped millions of dollars through click hijacking and advertisement replacement fraud.[361]

The Indictment is well drafted in accordance with the modus operandi of the scheme, covering a range of cyber offences.[362] These type of offences will soon

---

356 Section 3.5.
357 Section 4.4.4; Indictment para 2 at 2.
358 Section 4.4.4; Indictment para 3 at 3.
359 Section 4.4.4; Indictment 5.
360 Section 4.4.4; Indictment para 4 at 5-6.
361 Section 4.4.4; Indictment para 5 at 7.
362 Section 4.4.4.

and in the near future be the norm, and unless South Africa has similar Acts dealing specifically with these types of cyber offences, extraditions will be exigent.

6.4 Conclusion

The transnational nature of electronic evidence, exacerbated by porous international borders,[363] exposes the transient nature of e-crime and the ease in which fugitives from justice operate. The purpose of the Cybercrimes Act 19 of 2020, amongst others is to regulate jurisdiction in respect of cybercrimes. Jurisdiction must mean international jurisdiction, as the Act allows for the entering into agreements with foreign States to promote inhibitory measures in cybercrime, but in the same breath South Africa has not ratified the cybercrime convention and other conventions to give effect not only to the spirit of the Act, but also for the harmonisation of extradition procedures. An extradition involves the principle of specialty which means that the extradited person will be tried only for offences listed in the request, which is a rule of customary international law and which forms part of South African law.[364] Its absence, therefore, would be in violation of South African law.[365] South Africa has to align itself with international laws, precedents and treaties to be more effective in cybercrime extraditions.

The question of whether South Africa has adequate cyber laws, to fulfil its international obligations in respect of extraditions will be a challenge, bearing in mind that as the Cybersecurity Bill has been severed from the Cybercrimes Act. The empirical reverberation of the Cybercrimes Act on organisations and people are significant, and regrettably mostly fatalistic with regard to the curtailing of freedom and over criminalising the everyday acts with a computer.[366] The Cybercrimes Act has no reference to the Cybersecurity Bill. The delay in implementation as well as the lack of implementation is critical to the rule of law. Cybersecurity laws are not adequate to deal with economic espionage and

---

363 Section 2.5.
364 Section 4.5.
365 Section 4.5.
366 Section 3.3.

protection of Infrastructure, in respect of ransom ware attacks and paralysis of the infrastructure systems.[367]

The convolutions yoked with the challenges of prowess in the cybercrime sphere, have resulted in there being no prosecutions in terms of the ECT Act.[368] It dishearteningly appears that the law has not even been reactive to cybercrimes, as nothing happened, and going forward, a proactive slant in cybercrime prosecutions and extraditions is now dire. In order to achieve this, both legal and procedural challenges must be examined with a clear understanding of the context within which they emerge.[369]

The ramifications of all of these issues are that South Africa will rarely be the requesting state for cyber offences and will grapple with the complexity of extradition requests by requesting states until legislation is meaningfully integrated with global role players.

---

367 Section 5.2.2.
368 Section 3.5.
369 London, 'Comparative data protection and security law' 95.

7 Bibliography

7.1 Books

Bassiouni, *International Extradition*

Bassiouni MC, *International Extradition United States Law and Practice* (5th edn, Oxford University Press 2007)

Bingham, *The rule of law*

Bingham TH, *The rule of law* Part 1 (Penguin 2011)

Du Toit and others, *Commentary on the Criminal Procedure Act*

Du Toit E and others, *Commentary on the Criminal Procedure Act* (Juta 1993)

Dugard, Du Plessis and Katz, *International Law*

Dugard J, Du Plessis M and Katz A, *International Law: A South African Perspective* (Juta 2012)

Dugard J, *International Law: A South African Perspective* (4th edn, Juta 2011)

Holtzman, *Privacy Lost'*

Holtzman DH, *Privacy Lost: How Technology is Endangering your Privacy* (Jossey-Bass 2006)

Jahankhani and Hosseinian-far, 'Digital forensics education, training and awareness'

Jahankhani H and Hosseinian-far A, 'Digital forensics education, training and awareness', in Babak Akhgar, Andrew Staniforth, Francesca Bosco (eds), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Syngress 2014) Chapter 8, 91-100

Jahankhani, Al-Nemrat and Hosseinian-far, 'Cybercrime classification and characteristics'

Jahankhani H, Al-Nemrat A and Hosseinian-far A, 'Cybercrime classification and characteristics' in B Akhgar, A Staniforth and F Bosco

(eds), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Syngress 2014) Chapter 12 149-164

Jeffries and Apeh, 'Standard operating procedures for cybercrime investigations'

Jeffries S and Apeh E, 'Standard operating procedures for cybercrime investigations: a systematic literature review' in V Benson and J McAlaney, *Emerging Cyber Threats and Cognitive Vulnerabilities* (Academic Press 2020)

Jennings and Watts (eds), *Oppenheim's International Law*

Jennings R and Watts A (eds), *Oppenheim's International Law* (8th edn, Oxford University Press 1955)

Milton and Hunt, *Criminal Law and Procedure*

Milton J and Hunt MA, *South African Criminal Law and Procedure* (3rd edn, Juta 1996)

Oppenheim, *International Law*

Oppenheim L, *International Law* (8th edn, Longmans 1955)

Osborne, 'Information Security Laws and Regulations'

Osborne M, 'Information Security Laws and Regulations', in M Osborne (ed), *How to Cheat at Managing Information Security* (Syngress 2006) Chapter 4, 71-86

Schmitt, *Tallinn Manual 2.0 on the International Law*

Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations General* (2nd edn, Cambridge University Press 2017)

Shearer, *Extradition in International Law*

Shearer IA, *Extradition in International Law* (Manchester University Press 1971)

Shinder and Cross, 'Building the Cybercrime Case'

Shinder DL and Cross M, ‘Building the Cybercrime Case’ in DL Shinder and M Cross (eds), *Scene of the Cybercrime* (2nd edn, Syngress 2008) Chapter 14 653-691

Snyman, *Criminal Law*

Snyman CR, *Criminal Law* (5th edn, LexisNexis 2008)

Wang, *A Comparative Study of Cybercrime in Criminal Law*

Wang Q, *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe* (Wolf Legal 2016)

Wilhelm, ‘Ethics and Hacking’

Wilhelm T, ‘Ethics and Hacking’, in Thomas Wilhelm (ed), *Professional Penetration Testing: Creating and Learning in a Hacking Lab* (2nd edn, Syngress 2013) Chapter 2, 11-36

7.2 Dissertations/Thesis

London, ‘Comparative data protection and security law’

London RW, ‘Comparative data protection and security law: A critical evaluation of legal standards’ (PhD thesis University of South Africa 2013)

Maat, ‘Cyber-crime’

Maat SM, ‘Cyber-crime: a comparative law analysis’ (LLM dissertation, University of South Africa 2004)

Netshitangani, ‘An evaluation of the implementation of community policing’

Netshitangani NA, ‘An evaluation of the implementation of community policing in Westonaria’ (MA dissertation, University of South Africa 2018)

7.3 Journal articles

Basdeo, ‘Criminal and Procedural Legal Challenges’

Basdeo V, ‘Criminal and Procedural Legal Challenges of Identity Theft in the Cyber and Information Age’ (2017) 30 SAJCJ 363

Boister, ‘The trend to “universal extradition”’

Boister N, ‘The trend to “universal extradition” over subsidiary universal jurisdiction in the suppression of transnational crime’ (2003) 1 Acta Juridica 287

Botha, ‘Lessons from Harksen’

Botha N, ‘Lessons from Harksen: a closer look at the constitutionality of extradition in South African law’ (2000) 33 CILSA 274

Clough, ‘A World of Difference’

Clough J, ‘A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation Cybercrime’ (2014) 40 Monash ULR 698

Du Plessis, ‘The Pinochet cases and South African extradition law’

Du Plessis M, ‘The Pinochet cases and South African extradition law’ (2000) 16 SAJHR 669

Dugard, ‘Dealing with crimes of a past regime’

Dugard J, ‘Dealing with crimes of a past regime: Is amnesty still an option?’ (1999) 12 Leiden Journal of International Law 1001

Greenleaf and Georges, ‘The African Union’s Data Privacy Convention’

Greenleaf G and Georges M, ‘The African Union’s Data Privacy Convention: A Major Step Toward Global Consistency?’ (2014) 131 Privacy Laws and Business International Report 18

Johannessen, Klaaren and White, 'A motivation for legislation'

Johannessen L, Klaaren J and White J, 'A motivation for legislation on access to information' (1995) 112 SALJ 56

Katz, ‘The incorporation of extradition agreements’

Katz A, ‘The incorporation of extradition agreements’ (2003) 16 SACJ 311

Kerr, ‘Vagueness challenges to the Computer Fraud and Abuse Act’

Kerr OS, ‘Vagueness challenges to the Computer Fraud and Abuse Act’ (2010) 94 Minnesota Law Review 1561

Leonard, ‘What is extradition? Part 1’

Leonard E, ‘What is extradition? Part 1’ (2015) 108 Servamus Community-based Safety and Security Magazine 30-31

‘Leonard, ‘Extradition outgoing extraditions - Part 2’

Leonard E, ‘Extradition outgoing extraditions - Part 2’ (2015) 108 Servamus Community-based Safety and Security Magazine 30-31

Maillart, ‘The limits of subjective territorial jurisdiction’

Maillart JB, ‘The limits of subjective territorial jurisdiction in the context of cybercrime’ (2014) 40 ERA Forum 375

Marcu, ‘The Execution of the European Arrest Warrant’

Marcu EC, ‘The Execution of the European Arrest Warrant’ (2016) 65 The Juridical Current 132

Mokoena and Lubaale, 'Extradition in the absence of state agreements'

Mokoena UCA and Lubaale EC, 'Extradition in the absence of state agreements: Provisions in international treaties on extradition' (2019) 67 SA Crim Q 31

Mujuzi, ‘The South African International Co-Operation in Criminal Matters Act’

Mujuzi JD, ‘The South African International Co-Operation in Criminal Matters Act and the issue of evidence’ (2015) 48 De Jure 351

O’Shea, ‘Pinochet and Beyond: The International Implications of Amnesty’

O’Shea A, ‘Pinochet and Beyond: The International Implications of Amnesty’ (2000) 16 SAJHR 642

Roos, ‘The European Union’s General Data Protection Regulation (GDPR)'

Roos A, ‘The European Union’s General Data Protection Regulation (GDPR) and Its Implications for South African Data Privacy Law : An Evaluation of Selected’ (2020) CILSA 53

Snail SL, ‘An overview of South African e-consumer law’

Snail SL, ‘An overview of South African e-consumer law in the context of the Electronic Communications and Transactions Act (part 2)’ (2007) 15 Juta’s Business Law 54

Snyder, ‘Literature review as a research methodology’

Snyder H, ‘Literature review as a research methodology: An overview and guidelines’ (2019) 104 Journal of Business Research 333

Stein, ‘South Africa’s EU-Style Data Protection Law’

Stein P, ‘South Africa’s EU-Style Data Protection Law’ (2012) 12 Without Prejudice 48

Sutherland, ‘Governance of Cybersecurity’

Sutherland E, ‘Governance of Cybersecurity – The Case of South Africa’ (2017) 20 AJIC 83

Van der Berg, ‘Notes on an aspect of extradition'

Van der Berg J, ‘Notes on an aspect of extradition' (1987) 12 Journal for Juridical Science 202

Warbrick and McGoldrick, ‘Extradition Law Aspects’

Warbrick C and McGoldrick D, ‘Extradition Law Aspects of Pinochet 3’ (1999) 48 International and Comparative Law Quarterly 958

Watney, ‘A South African perspective on mutual legal assistance’

Watney M, ‘A South African perspective on mutual legal assistance and extradition in a globalized world’ (2012) 15 PELJ 292

Watney, ‘Unreasonable delays in criminal trials’

Watney MM, ‘Unreasonable delays in criminal trials and the remedy of a permanent stay of prosecution *Zanner v Director of Public Prosecutions, Johannesburg* 2006 (2) SACR 45 (SCA)’ (2007) 45 TSAR 422

7.4 Newspaper articles

Evanoff and Roberts, ‘A sputnik moment for artificial intelligence geopolitics’

Evanoff K and Roberts M, ‘A sputnik moment for artificial intelligence geopolitics’ *The Internationalist* (7 September 2017)

Hanson, ‘When laws are not enforced, anarchy follows’

Hanson VD, ‘When laws are not enforced, anarchy follows’ *Tribune News Service* (3 November 2018)

Hosken, ‘Millions in SA at risk after data theft’

Hosken G, ‘Millions in SA at risk after data theft’ *Sunday Times* (South Africa, 13 September 2020)

Manaka, ‘Understanding the impact of the Regulation of Interception’

Manaka C, ‘Understanding the impact of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002’ *Mondaq* [16 December 2010]

Pinnock, ‘What recent data breaches tell us about cybersecurity’

Pinnock B, ‘What recent data breaches tell us about cybersecurity in South Africa’ *BusinessTech* (16 September 2020)

Ramjathan-Keogh, ‘South Africa, Apartheid, Crimes against humanity and the Rule of Law’

Ramjathan-Keogh K, ‘South Africa, Apartheid, Crimes against humanity and the Rule of Law: Quo Vadis’ *Daily Maverick* (21 February 2020)

Satariano, ‘What the G.D.P.R., Europe’s Tough New Data Law, Means for You’

Satariano A, ‘What the G.D.P.R., Europe’s Tough New Data Law, Means for You’ *The New York Times* (New York, 6 May 2018)

7.5 Case law

Advocaten voor de Wereld VZW v Leden van de Ministerraad Case C-303/05

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC [2021] ZACC 3

Bell v S [1997] 2 All SA 692 (EC)

Bell v State A101/2014 ZAGPHC

Director of *Public Prosecutions*, *Western Cape v Kouwenhoven* (A181/2020) [2020] ZAWCHC 185 (23 December 2020)

Doma v S (2012/A447) [2013] ZAGPJHC 116 (21 May 2013)

Ex parte Pinochet Ugarte (No 3) [1999] 2 WLR 824; [2000] 1 AC 147 (HL)

Geuking v President of the Republic of South Africa (CCT35/02) [2002] ZACC 29; 2003 (3) SA 34 (CC)

Harksen v President of RSA 2000 (2) SA 825 (CC)

Harksen v President of the Republic of South Africa and Others (CCT 41/99) [2000] ZACC 29; 2000 (2) SA 825 (CC); 2000 (1) SACR 300; 2000 (5) BCLR 478 (30 March 2000)

Hoho v The State (493/05) [2008] ZASCA 98 (17 September 2008)

Inc v UEJF and LICRA USA001R

Kouwenhoven v DPP (Western Cape) and Others (288/2021) [2021] ZASCA 120 (22 September 2021)

Kouwenhoven v Minister of Police (1477/2018) [2019] ZAWCHC 154; [2019] 4 All SA 768 (WCC) (19 September 2019)

Mackeson v Minister of Information, Immigration and Tourism [1980] (1) SA 747 (ZR)

McCarthy v Additional Magistrate, Johannesburg [2000] (2) SACR 542 (SCA)

Minister of Justice v Additional Magistrate, Cape Town 2001 para 33; (*Director of Public Prosecutions: Cape of Good Hope v Trevor Claud Robinson* Case No 15/04)

Mohamed and Another v President of the Republic of South Africa and Others (CCT 17/01) [2001] ZACC 18; 2001 (3) SA 893 (CC); 2001 (7) BCLR 685 (CC) (28 May 2001)

Palazzolo v Minister of Justice and Constitutional Development (4731/2010) [2010] ZAWCHC 422 (14 June 2010)

Palazzolo v Minister of Justice and Constitutional Development (4731/2010) [2010] ZAWCHC 422 (14 April 2011)

Patel v National Director of Public Prosecutions (NDPP) (838/2015) [2016] ZASCA 191; 2017 (1) SACR 456 (SCA) (1 December 2016)

Patel v S (A101/2014) [2015] ZAGPJHC 188; [2015] 4 All SA 382 (GJ); 2016 (2) SACR 141 (GJ) (18 August 2015)

President of the Republic of South Africa and Others v Quagliani; President of the Republic of South Africa and Others v Van Rooyen and Another; Goodwin v Director-General, Department of Justice and Constitutional Development and Others (CCT24/08, CCT52/08) [2009] ZACC 1; 2009 (4) BCLR 345 (CC); 2009 (2) SA 466 (CC) (21 January 2009)

S v Basson [2005] ZACC 10; 2007 (3) SA 582 (CC); 2005 (12) BCLR 1192 (CC)

S v Ebrahim (279/89) [1991] ZASCA 3; 1991 (2) SA 553 (AD); [1991] 4 All SA 356 (AD) (26 February 1991)

S v Okah [2018] ZACC Case CCT 315/16 and CCT 193/17 CCT 315/16

S v Speedie (444/83) [1985] ZASCA 1; [1985] 2 All SA 112 (A) (12 March 1985)

Saliu v S (2014/A262) [2015] ZAGPJHC 175 (25 August 2015)

Smit v Minister of Justice and Correctional Services and Others [2020] ZACC 29

7.6 Legislation

7.6.1 South Africa

Citizenship Act 88 of 1995
Constitution of the Republic of South Africa Act 108 of 1996
Constitution of the Republic of South Africa, 1996

Correctional Services Act 111 of 1998

Criminal Procedure Act 51 of 1977

Cybercrimes Act 19 of 2020

Cybercrimes and Cybersecurity Bill Republic of South Africa, 2017

Electronic Communications and Transactions Act 25 of 2002

Electronic Communications and Transactions Amendment Bill, 2012

Extradition Act 67 of 1962

Extradition Act 67 of 1962

Extradition Amendment Act 77 of 1996

Financial Intelligence Centre Act 38 of 2001

General Law Amendment Act 62 of 1955

Identification Act 68 of 1997

Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002

Intelligence Services Act 38 of 1994

International Co-operation in Criminal Matters Act 75 or 1996

National Prosecuting Authority Act 32 of 1998

Police Service Act 68 of 1995

Prevention and Combating of Corrupt Activities Act 12 of 2004

Prevention of Organised Crime Act 121 of 1998

Promotion of Access to Information Act 2 of 2000

Protection from Harassment Act 17 of 2011

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Royal Executive Functions and Seals Act 70 of 1934

South African Police Service Act 68 of 1995

7.6.2 Namibia

International Co-operation in Criminal Matters Act 9 of 2000

7.6.3 Canada

Privacy Act, 1985 (Canada)

7.6.4 United Kingdom

British Extradition Act, 1870
British Fugitive Act, 1881
Computer Misuse Act, 1990
Copyright, Designs and Patents Act, 1988
Data Protection Act, 1984
Data Protection Act, 2018
Fraud Act, 2006
Investigatory Powers Act, 2016
Network and Information Systems Regulation, 2018
Police Act, 1997
Police and Justice Act, 2006
Proceeds of Crime Act, 2002
Public General Acts 1994
Theft Act, 1978

7.6.5 United States

Computer Fraud and Abuse Act 1984
Economic Espionage Act, 1996
Freedom Act, 2020
National Information Infrastructure Protection Act, 1996
Patriot Act, 2001

7.7 Government publications

General Notice R458 in Government Gazette 23708 of 18 May 2007 (Electronic Communications and Transactions Act 25 of 2002)

General Notice 871 in Government Gazette 40487 of 9 December 2016 (Cybercrimes and Cybersecurity Bill Republic of South Africa 2017)

Government Gazette 17589 of 20 November 1996 (Extradition Amendment Act 77 of 1996)

Government Gazette 7100 of 29 June 2001 (Extradition and Mutual Legal Assistance in criminal matters treaties)

Government Gazette 23708 of 2 August 2002 (Electronic Communications and Transactions Act 25 of 2002)

Government Gazette 24872 of 13 May 2003 Vol 455 (European Convention on Extradition (and the Two Additional Protocols))

Government Gazette 31844 of 6 February 2009 Vol 451 (Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002)

Government Gazette 40487 of 9 December 2016 (Cybercrimes and Cybersecurity Bill Republic of South Africa)

Government Gazette 40978 of 14 July 2017 (Extradition Treaty Between the Republic of South Africa and the Argentine Republic)

WTO 'Agreement on Trade-Related Aspects of Intellectual Property Rights' <https://www.wto.org/english/docs_e/legal_e/27-trips.pdf> accessed 10 January 2021

7.8 International instruments

Directive 95/46/EC

> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046> (No longer in force, date of end of validity: 24/05/2018) accessed 8 March 2021

European Convention on Extradition - Paris, 13.Xii.1957

> European Convention on Extradition - Paris, 13.Xii.1957, European Treaty Series No 24 <https://rm.coe.int/1680064587> accessed 29 April 2020

European Treaty Series No 182

> European Convention on Mutual Assistance in Criminal Matters (Second Additional Protocol) 'European Treaty Series No 182' <https://rm.coe.int/16800 8155e> accessed 13 December 2020

European Treaty Series No 185

Explanatory Report to the Convention on Cybercrime (European Treaty Series No 185) <https://rm.coe.int/16800cce5b> accessed 4 May 2020

European Treaty Series No 30

European Convention on Mutual Assistance in Criminal Matters (European Treaty Series No 30) <https://rm.coe.int/16800656ce> accessed 14 January 2021

Ratification of Accession (4 June 2001)

Ratification of Accession (4 June 2001) <https://bch.cbd.int/help/topics/en/Ratification%20and%20Accession.html> accessed 14 May 2020

Regulation (EU) 2016/679

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <http://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 8 March 2021

T-CY Assessment Report

T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime (2-3 December 2014) <https://rm.coe. int/16802e726c> accessed 12 May 2020

United Nations (UN) Report March 2016 ‘International Covenant on Civil and Political Rights’

United Nations (UN) Report March 2016 ‘International Covenant on Civil and Political Rights’ <http://docstore.ohchr.org/SelfServices/FilesHandler.Ashx?Enc=6QkG1d%2fPPRiCAqhKb7yhsowwsSwFehBWX2ZjedBh4%2f811AqGyI2MTdng6xdE8vcB81uWeU1SfkzAjkFApm4n4sVMY4cvhDsmlet3UuCiWMpSKAPdJOaa%2bhTfv%2fQXEkwx> accessed 20 October 2020

Vienna Convention on the Law of Treaties (23 May 1969)

Vienna Convention on the Law of Treaties (23 May 1969) <https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf> accessed 10 January 2021

7.9 Internet sources

Ameer-Mia and Shacksnovis, 'Cybercrimes Bill – A positive step'

Ameer-Mia F and Shacksnovis L, 'Cybercrimes Bill – A positive step towards the regulation of cybercrimes in South Africa' (*Technology and Sourcing*, 13 February 2019) <https://www.cliffedekkerhofmeyr.com/export/sites/cdh/en/news/publications/2019/technology/downloads/Technology-Sourcing-Alert-13-February-2019.pdf> accessed 6 June 2020

ACPO, 'Good Practice Guide for Digital Evidence'

ACPO (Association of Chief Police Officers), 'Good Practice Guide for Digital Evidence' (July 2007 and subsequently revised in November 2009 and March 2012) <https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf> accessed 18 August 2020

AU, 'Convention on Cyber-security and Personal Data Protection'

AU, 'Convention on Cyber-security and Personal Data Protection' (27 July 2014) <https://au.int/sites/default/files/treaties/29560-treaty-0048__african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf> accessed 6 June 2020

BAILII, 'England and Wales High Court (Administration Court) Decisions'

BAILII, 'England and Wales High Court (Administration Court) Decisions' (20 January 2021) <https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Admin/2021/53.html&query=(josse)+AND+(extradition)> accessed 15 July 2021

Baker, 'What does the newly signed "Convention 108+" mean for UK adequacy?'

Baker J, ‘What does the newly signed “Convention 108+” mean for UK adequacy?’ (*The Privacy Advisor*, 30 October 2018) <https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/> accessed 8 March 2021

BBC News, ‘Ransomware hits Johannesburg electricity supply’

BBC News, ‘Ransomware hits Johannesburg electricity supply’ (26 July 2019) <https://www.bbc.com/news/technology-49125853> accessed 5 June 2020

Bregmans, ‘Criminal Defamation’

Bregmans, ‘Criminal Defamation’ (26 June 2019) <https://www.bregmans.co.za/criminal-defamation/> accessed 10 March 2021

British Exit, ‘The withdrawal of the United Kingdom from the European Union’

British Exit, ‘The withdrawal of the United Kingdom from the European Union’ (2021) <https://www.google.com/search?q=brexit+meaning&rlz=1C1GCEU_enZA821ZA822&oq=br&aqs=chrome.0.69i59j69i57j69i59j0i67l2j69i60l3.2671j0j7&sourceid=chrome&ie=UTF-8> accessed 15 July 2021

Burgess, ‘Do cybercriminals ever get extradited?’

Burgess C, ‘Do cybercriminals ever get extradited?’ *Security Boulevard* (13 April 2018) <https://securityboulevard.com/2018/04/do-cybercriminals-ever-get-extradited> accessed 14 September 2020

Business Insider SA, ‘Hackers on the dark web love South Africa’

Business Insider SA, ‘Hackers on the dark web love South Africa - here’s why we suffer 577 attacks per hour’ (3 June 2020) <https://www.businessinsider.co.za/sa-third-highestnumber-of-cybercrime-victims-2020-6> accessed 5 June 2020

BusinessTech, ‘Stay vs leaving the country – what young South African workers plan to do’

BusinessTech, ‘Stay vs leaving the country – what young South African workers plan to do’ (12 March 2021)

<https://businesstech.co.za/news/business/475468/stay-vs-leaving-the-country-what-young-south-african-workers-plan-todo/?utm_source=everlytic&utm_medium=newsletter&utm_campaign=businesstech> accessed 12 March 2021

Citizens Information, ‘Extradition to and from Ireland’

Citizens Information, ‘Extradition to and from Ireland’ (13 January 2021) <https://www.citizensinformation.ie/en/justice/arrests/extradition_to_and_from_ireland.html#l414a7> accessed 15 July 2021

Cliffe Dekker Hofmeyr Inc, 'The International Comparative Legal Guide to: Cybersecurity 2019'

Cliffe Dekker Hofmeyr Inc, 'The International Comparative Legal Guide to: Cybersecurity 2019' (2nd edn 2019) Chapter 29 185-191 <https://www.mhmjapan.com/content/files/00032671/The%20International%20Comparative%20Legal%20Guide%20to%20Cybersecurity%202019%20-%20Japan%20Chapter.pdf> accessed 20 March 2020

Collins, ‘European Extradition after Brexit: What now?’

Collins L, ‘European Extradition after Brexit: What now?’ (25 January 2021) <https://www.5sah.co.uk/knowledge-hub/news/2021-01-27/high-court-clarifies-status-of-ongoing-eaws-post-brexit> accessed 15 July 2021

Computer Crime Research Center, ‘Putin Defies Convention on Cybercrime’

Computer Crime Research Center, ‘Putin Defies Convention on Cyber-crime’, (online) (28 March 2008) <https://www.crime-research.org/news/28.03.2008/3277/> accessed 15 January 2021

Constitutional Court of South Africa, ‘*AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services*; *Minister of Police v AmaBhungane Centre for Investigative Journalism NPC*’ Case CCT278/19 & CCT279/19 [2021] ZACC 03’

Constitutional Court of South Africa, ‘*AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional*

Services; *Minister of Police v AmaBhungane Centre for Investigative Journalism NPC*' Case CCT278/19 & CCT279/19 [2021] ZACC 03 <https://www.concourt.org.za/ index.php/judgement/383-amabhungane-centre-for-investigative-journa lism-npc-and-another-v-minister-of-justice-and-correctional-services-and-others-minister-of-police-v-amabhungane-centre-for-investigative-journa lism-npc-and-others-cct278-19-cct279-19> accessed 8 March 2021

Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'

Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Strasbourg, 28 January 1981) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> accessed 8 March 2021

Council of Europe, 'Convention on Cybercrime: Chart of Signatures and Ratification of Treaty 185'

Council of Europe, 'Convention on Cybercrime: Chart of Signatures and Ratification of Treaty 185' (23 November 2001) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures> accessed 15 May 2021

Council of Europe, 'List of Treaties'

Council of Europe, 'List of Treaties' (1 May 20212) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/209?module=signatures-by-treaty&treatynum=185> accessed 12 May 2020

Council of the European Union, 'Council Framework Decision'

Council of the European Union, 'Council Framework Decision' (2002/584/JHA) (13 June 2002) on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision; International Law & Order 1; Official Journal of the European Communities <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584> accessed 30 August 2020

Department of Justice and Constitutional Development, ‘International Legal Obligations’

Department of Justice and Constitutional Development, ‘International Legal Obligations’ <https://www.justice.gov.za/ilr/mla.html> accessed 20 July 2020

EDPB, ‘Baden-Württemberg supervisory authority issues first German GDPR fine’

European Data Protection Board (EDPB), ‘Baden-Württemberg supervisory authority issues first German GDPR fine’ (22 November 2018) <https:// edpb.europa.eu/news/national-news/2018_en> accessed 6 June 2020

EDPB (European Data Protection Board), ‘The CNIL’s restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC’

EDPB (European Data Protection Board), ‘The CNIL’s restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC’ (21 January 2019) <https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en> accessed 31 May 2020

EUR-Lex, ‘Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community’

EUR-Lex, ‘Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part’ L 444/14 - Official Journal of the European Union 31.12.2020: part three: Law Enforcement and Judicial Cooperation in Criminal Matters 300 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.444.01. 0014. 01.ENG> accessed 15 July 2021

EUROJUST, ‘Cybercrime Judicial Monitor’ para 3.1 Selected Court Rulings 11.

EUROJUST, ‘Cybercrime Judicial Monitor’ para 3.1 Selected Court Rulings 11 (Court of First Instance Antwerp, Section Mechelen, ME20.F1.105151-12, Belgium, 27 October 2016) (December 2017) <https://www.eurojust.eu ropa.eu/sites/default/files/Publications/Reports/2017-12_CJM-3_EN.pdf> accessed 25 May 2020

European Convention on Cybercrime, ‘Budapest, 23.X1.2001 European Treaty Series - No 185’

European Convention on Cybercrime, ‘Budapest, 23.X1.2001 European Treaty Series - No 185’ <https://Rm.Coe.Int/1680064587> accessed 29 April 2020

Financial Intelligence Centre, ‘Legislation’ <https://www.fic.gov.za/Resources/ Pages/Legislation.aspx> accessed 12 March 2021

Financial Intelligence Centre, ‘Legislation’ <https://www.fic.gov.za/Resour ces/Pages/Legislation.aspx> accessed 12 March 2021

General Data Protection Regulation, ‘Data Protection Guide’ (27 April 2016)

General Data Protection Regulation, ‘Data Protection Guide’ (27 April 2016) <https://www.google.com/search?q=eu+general+data+protection+regulati on&rlz=1C1CHBD_enZA770ZA770&oq=EU+General+Data+Protection+R egulation&aqs=chrome.0.0i457j0j46j0l5.1467j0j7&sourceid=chrome&ie=U TF-8> accessed 10 June 2020

Gercke, ‘Understanding cybercrime: phenomena, challenges and legal response’

Gercke M, ‘Understanding cybercrime: phenomena, challenges and legal response’ (November 2014) <https://www.itu.int/en/ITU-D/Cybersecurity/ Documents/cybercrime2014.pdf> accessed 30 December 2020

Grierson, Rankin and O’Carroll, ‘UK to withdraw from European arrest warrant’

Grierson J, Rankin J and O’Carroll L, ‘UK to withdraw from European arrest warrant’ *The Guardian* (United Kingdom, 27 February 2020)

<https://www. theguardian.com/uk-news/2020/feb/27/uk-to-withdraw-from-european-arre st-warrant> accessed 15 July 2021

Hayes and Drury, 'Cybersecurity in United Kingdom'

Hayes J and Drury M, 'Cybersecurity in United Kingdom (England & Wales)' (*Lexology*, 23 December 2019) <www.lexology.com›library›detail›g=0926 2dc8-60...> accessed 21 March 2021

International Law: The Importance of Extradition

International Law: The Importance of Extradition <https://www.govinfo.gov/content/pkg/CHRG-106hhrg63238/html/CHRG-106hhrg63238.htm> accessed 20 April 2020

Kervick, 'Extradition post-Brexit: the TCA at a glance'

Kervick A, 'Extradition post-Brexit: the TCA at a glance' (29 January 2021) <https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/extradition-post-brexit-the-tca-at-a-glance> accessed 15 July 2021

Legal Sidebar, 'USA Freedom Act Reinstates Expired USA Patriot Act Provisions but Limits Bulk Collection'

Legal Sidebar, 'USA Freedom Act Reinstates Expired USA Patriot Act Provisions but Limits Bulk Collection' (6 April 2015) <https://fas.org/sgp/crs/ intel/usaf-rein.pdf> accessed 2 July 2021

Mbuvi, 'African States Urged to Ratify Budapest Cybercrime Convention'

Mbuvi D, 'African States Urged to Ratify Budapest Cybercrime Convention' (10 October 2011) <https://www.csoonline.com/article/2129762/african-states-urged-to-ratify-budapest-cybercrime-convention.html> accessed 13 January 2021

Michalsons, 'Cybercrimes Act in South Africa – Overview and Read'

Michalsons, 'Cybercrimes Act in South Africa – Overview and Read' (date unknown) <https://www.michalsons.com/blog/cybercrimes-and-cybersecuri ty-bill-the-cac-bill/16344> accessed 2 June 2020

Michalsons, ‘Guide to the ECT Act in South Africa’

Michalsons, ‘Guide to the ECT Act in South Africa’ (25 September 2008) <https://www.michalsons.com/blog/guide-to-the-ect-act/81> accessed 6 August 2020

NACDL, 'CFAA Background'

National Association of Criminal Defence Lawyers (NACDL), 'CFAA Background' (10 March 2020) <https://www.nacdl.org/Content/CFAABackground> accessed 15 May 2021

NACDL, ‘Computer Fraud and Abuse Act (CFAA)’

National Association of Criminal Defence Lawyers (NACDL), ‘Computer Fraud and Abuse Act (CFAA)’ <https://www.nacdl.org/Landing/ComputerFraudandAbuseAct> accessed 15 May 2021

National Prosecuting Authority of South Africa, 'Justice in our society, so that people can in live in freedom and security'

National Prosecuting Authority of South Africa, 'Justice in our society, so that people can in live in freedom and security' (2021) <https://www.npa.gov.za/> accessed 28 May 2021

Otto, ‘Court blow for alleged mafia boss’

Otto J, ‘Court blow for alleged mafia boss’ (21 December 2012) <https://www.iol.co.za/news/court-blow-for-alleged-mafia-boss-1444016> accessed 6 May 2020

Parliament, ‘Justice Committee wants urgent implementation of full POPIA’

Parliament, ‘Justice Committee wants urgent implementation of full POPIA’ (12 May 2020) <https://www.parliament.gov.za/press-releases/justice-com mittee-wants-urgent-implementation-full-popia> accessed 25 May 2020

Patel and Bharadwaj, ‘Budapest Convention on Cyber Crime’

Patel DA and Bharadwaj S, ‘Budapest Convention on Cyber Crime’ (2020) <http://studymaterial.unipune.ac.in:8080/jspui/bitstream/123456789/4798/1/BUDAPEST%20CONVENTION%20ON%20CYBER%20CRIME-converted.pdf> accessed 26 May 2020

Perkins, ‘Shedding light on the hidden epidemic of police suicide in South Africa’

Perkins G, ‘Shedding light on the hidden epidemic of police suicide in South Africa’ (3 February 2016) <https://theconversation.com/shedding-light-on-the-hidden-epidemic-of-police-suicide-in-south-africa-53318> accessed 31 December 2020

Pinteală, ‘Legal aspects of the European arrest warrant’

Pinteală G, ‘Legal aspects of the European arrest warrant’ Quaestus Multi-disciplinary Research Journal Legal 183 <https://www.quaestus.ro/wp-content/uploads/2012/03/pinteala2.pdf> accessed 13 February 2021

Ramaphosa, 'Commencement of certain sections of the Protection of Personal Information Act, 2013'

Ramaphosa C, 'Commencement of certain sections of the Protection of Personal Information Act, 2013' (22 June 2020) <http://www.thepresidency. gov.za/press-statements/commencement-certain-sections-protection-per sonal-informa tion-act%2C-2013> accessed 22 June 2020

Ramluckan, ‘The Applicability of the Tallinn Manuals to South Africa’

Ramluckan T, ‘The Applicability of the Tallinn Manuals to South Africa’ 14th International Conference on Cyber Warfare and Security (ICCWS) (2019) 348-355 <https://www.proquest.com/openview/ac4cc9f3edd6ada5ae1cfe838cb65e68/1?pq-origsite=gscholar&cbl=396500> accessed 12 May 2020

Right2Know Admin, ‘State security: hands off the internet! No to spooks regulating social media’

Right2Know Admin, ‘State security: hands off the internet! No to spooks regulating social media’ (8 April 2019) <http://www.r2k.org.za/2017/03/07/tate-security-hands-off-the-internet-no-to-spooks-regulating-social-media/> accessed 23 December 2020

Right2Know Campaign, ‘Hands Off Social Media’

Right2Know Campaign, ‘Hands Off Social Media’ <https://awethu.amandla. mobi/petitions/handsoffoursocialmedia> accessed 23 December 2020

Right2Know Campaign, ‘R2K protests against Rica surveillance’

Right2Know Campaign, ‘R2K protests against Rica surveillance’ News24 (26 April 2016) <https://www.news24.com/News24/right2know-protests-against-rica-surveillance-20160426> accessed 23 December 2020

Right2Know Campaign, ‘R2K submission on the Cybercrimes Bill’

Right2Know Campaign, ‘R2K submission on the Cybercrimes Bill’ (8 April 2017) <https://www.R2k.Org.Za/2017/08/11/R2k-Submission-on-the-Cyber crimes-Bill-2017> accessed 23 December 2020

Sharma, ‘Legislation Related to Cyber-Crimes in United Kingdom’

Sharma R, ‘Legislation Related to Cyber-Crimes in United Kingdom’ (December 2020) <https://www.researchgate.net/publication/347439774_Legislation_Related_to_Cyber_Crimes_in_United_Kingdomouth.Ac.Uk> accessed 15 January 2021

Sithole, ‘Policing Frameworks, Policing Systems, Policing Strategies, and Policing Models within the South African Context’

Sithole VE, ‘Policing Frameworks, Policing Systems, Policing Strategies, and Policing Models within the South African Context’ (Paper prepared for the National South African Police Services Colloquium in Pretoria 7th– 9th February 2017) <https://www.saps.gov.za/resource_centre/publications/dr_sithole_policing_frameworks_systems_and_stratetgies.pdf> accessed 12 May 2020

Smit, ‘Criminal law on cyber-crime in the Netherlands’

Smit AMG, ‘Criminal law on cyber-crime in the Netherlands’ (Preparatory Colloquium Helsinki (Finland), 10-12 June 2013. Section IV: International Criminal Law) <http://www.penal.org/sites/default/files/files/RH-11.pdf> accessed 15 January 2020

The United States Attorney’s Office, ‘*United States v Vladimir Tsastsin* Et Al 11 CR 878’

The United States Attorney’s Office, ‘*United States v Vladimir Tsastsin* Et Al 11 CR 878’ (9 November 2011) <https://www.justice.gov/usao-sdny/programs/victim-witness-services/united-states-v-vladimir-tsastsin-et-al-11-cr-878> accessed 15 May 2021

The USA Freedom Act

The USA Freedom Act <https://www.leahy.senate.gov/imo/media/doc/USA%20FREEDOM%20One-Pager%20-final.pdf> accessed 2 July 2021

TREATY - ETS 108+, ‘128th Session of the Committee of Ministers’

TREATY - ETS 108+, ‘128th Session of the Committee of Ministers’ (Elsinore, Denmark, 17-18 May 2018) Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf> accessed 8 March 2021

Turianskyi, ‘Balancing Cyber Security and Internet Freedom in Africa’

Turianskyi Y, ‘Balancing Cyber Security and Internet Freedom in Africa’ *Africa Portal* (31 January 2018) <https://www.africaportal.org/publications/balancing-cyber-security-and-internet-freedom-africa/> accessed 6 June 2020

UK Statutory Instruments 2018 No 506 (Network and Information Systems Regulations 2018) (NISR)

UK Statutory Instruments 2018 No 506 (Network and Information Systems Regulations 2018) (NISR) <https://www.legislation.gov.uk/uksi> accessed 8 March 2021

UN General Assembly, ‘Convention Relating to the Status of Refugees’

UN General Assembly, ‘Convention Relating to the Status of Refugees’ (28 July 1951) Vol 189, article 3 (available at <https://treaties.un.org/Pages/ViewDetailsII.aspx?src=TREATY&mtdsg_no=V-2&chapter=5&Temp=mtdsg2&clang=_en> accessed 30 April 2021

UN General Assembly, ‘Model Treaty on Extradition: resolution / adopted by the General Assembly’

UN General Assembly, ‘Model Treaty on Extradition: resolution / adopted by the General Assembly’ (14 December 1990) A/RES/45/116 <https://www.refworld.org/docid/3b00f18618.html> accessed 7 June 2020

UK Statutory Instruments, Explanatory Memorandum to the Network and Information Systems Regulations (NISR), 2018 No 506

UK Statutory Instruments, Explanatory Memorandum to the Network and Information Systems Regulations (NISR), 2018 No 506 <https://assets.publishing.service.gov.uk/media/5c7fb16940f0b6332d0ecf66/Network_EM.pdf> accessed 8 March 2021

Valcke, ‘The Rule of Law’

Valcke A, ‘The Rule of Law: Its Origins and Meanings (A short guide for practitioners)’ (1 March 2012) <http://ssrn.com/abstract=2042336> accessed 14 April 2020