"Recent Developments in South African law and International Law to fight computer crime, and the effectiveness of these developments. " - Adv. Aiden Darrel Maharaj

Table of Contents

A. Introduction

The General Assembly Resolution 60 of 177 of the United Nations was adopted in order to reaffirm the importance of global cooperation in the fight against computer crime. This resolution acknowledged that computer and telecommunication technologies are extremely vulnerable to criminal exploitation.[1] This paper will highlight that despite recent developments in the detection of cybercrime, the law has not provided an effective universal response to this global problem.

B. The extent of cyber crime

AshleyMadison.com, an adultery dating website based in Canada, was recently unlawfully infiltrated. An online article "Cyber Hacking, a Costly Affair"[2] illustrated the magnitude of Cybercrime.

Hackers were using the sensitive content to blackmail AshleyMadison.com threatening to disclose confidential information, of 37 million subscribers including South Africans. It was also reported that the impact of Cybercrime on South African was estimated at more than R5, 8 billion annually. It was also reported that the leading causes of cybercrime are disgruntled employees, negligence of the part of organisations or individuals, competitors and hackers.

[1] http://www.un.org/events/11thcongress/

[2] http://www.enca.com/life/Cyber-hacking-costly-affair (Date of use: 26 August 2015)

The AshleyMadison.com incident is a classic illustration of the abuse of the internet across multiple international jurisdictions.

In May 2015 the United States Federal Court imposed two life sentences on Ross Ulbricht for masterminding and operating Silk Road, an anonymous online emporium which allowed users to secretly trade illicit goods and malicious software designed for hacking, using the digital currency bitcoin[3] . It is estimated that Silk Road had electronically facilitated the sale $213 million of illicit goods. A five year term of imprisonment for conspiracy to commit computer hacking was ordered to run concurrently with the life imprisonment for the dealing of Drugs. The penalty imposed in the Silk Road saga highlight stark disproportionality in sentences imposed for traditional non computer-related crimes and computer related crimes.

C. The challenges associated with defining crimes associated with computers

Casssim succinctly opines that Computers can be considered to be the Subject or the Object in the commission of computer crime[4]. It is the Subject in the commission of offences where the physical Computer or its operating systems are targeted for theft or malicious destruction. Computers could also be utilised as an Object or as an Instrument for commission of a multitude of nefarious acts including fraud, terrorism, unauthorised appropriation and manipulation of personal and copyrighted material. The challenge is that consensus has not been reached how Computer Crime ought to be defined[5].

The United Nations developed two definitions in connection with computers.[6]

"(1) Cybercrime in a narrow sense (Computer crimes) covers any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. (2) Cybercrime in the broader sense (Computer related crimes) covers any illegal behaviour committed by means of or in relation to a computer system or networks including such crimes as illegal possession and offering or distributing information by means of a computer system or network"

Van der Merwe opines that he has had a Damascus conversion in respect of his approach toward computer crime. He has shifted his emphasis away from the computer hardware with a greater emphasis now being on the content of the computer[7]. Van der Merwe maintains that Data is the true legal interest, in need of protection and has proposed the following definition: "Computer crime covers all sets of circumstances where electronic data processing forms the means for the commission and or the object or represents the basis for the suspicion that an offence has been committed."[8] He opines that "Computer crime" is a

[3] Allen http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11640200/Silk-Road-founder-Ross-Ulbricht-sentenced-to-life-in-prison.html (Date of use: 3 September 2015)
[4] Cassim 2011 XILV CILSA 124
[5] Cassim ((n4 above) 124
[6] Gercke *Understanding Cybercrime*: 26
[7] Van der Merwe *Information Law* 63
[8] Van der Merwe 2007 (70) THRHR 310

dated concept and focus should shift towards new concepts of "Information and Computer Technology (ICT)", "data crime" and "data protection".

I align myself with the opinion of Van der Merwe that the significance of defining Computer Crime should be to preserve the integrity of Data.

D. The South African Developments

South African computer law has seen the development in the extension of the definition of crimes by the courts and the legislatures' enactment of statutory offences.

Computer crimes do not comfortably fit into the traditional definitions of statutory and common law crimes.

Prior to cyber legislation South African courts categorised misrepresentations committed electronically as Fraud.[9] However the principle of *nullem crimen sine lege* restricts judicial extension of the common law[10]. Hence a statutory framework was necessary to legislate against crimes, committed electronically that did not fit with the definition of traditional crimes.

In the digital age of computers, Data is incorporeal property as it is a digital magnetic molecule.[11] The nature of Data makes it difficult to be subjected to the traditional common law offence of Theft[12]. Theft is committed when the unlawful and intentional appropriation of movable corporeal property occurs[13]. In *S v Ndebele*[14] the court extended the common law to include the theft of electricity an incorporeal electron. Snyman[15] criticises this interpretation and maintains that theft can only be committed in terms of corporeal property and maintain that the courts should not usurp the roll of the legislature.

In *S v Howard*[16], prior to the enactment of cyber legislation, the South African courts extended the common law crime of malicious injury to property to include the unlawful access, corruption and erasure of data. During sentencing the court used the penalty provisions of the Electronic Communications and Transactions Act, Act 25 of 2002 (hereinafter referred to as ECT Act) as a guideline. (The aforementioned Act was not in operation, at the time of the commission of the offence.) The court imposed upon the accused a lenient sentence of 5 years imprisonment for an offence which had resulted in a loss of R57 million Rand.[17]

The ECT Act was enacted to prevent the abuse of information systems, unauthorised access to data, interception or interference with data, computer related extortion, fraud and

[9] *S v Van Berg* 1991 1 SACR 104 (T) at 106
[10] Van der Merwe Information Law 63
[11] Maat Cyber Crime: A Comparative Law Analysis 2004 103-108
[12] Watney TSAR 2005-3 608
[13] Snyman *Criminal Law* 475
[14] 2012 (1) SACR 245 (GSJ)
[15] Snyman *Criminal Law* 483
[16] *The State v Howard* Unreported case number 41/258/02 Johannesburg Regional Magistrates Court
[17] Watney TSAR 2005-3 603

forgery. Section 86(1) criminalises unauthorised access and interception of data. Section 86 (2) criminalised the abuse and integrity of the data. Section 86 (3) and (4) criminalises the possession and use of devices to override security used to protect information systems. Section 86 (5) criminalises acts that compromise information systems. Section 87 criminalises computer related extortion, fraud and forgery. Section 90 provides for extended jurisdiction where an offence was committed outside but the impacts is felt within the Republic on South Africa.

Section 90 enables the perpetrators in the Ashley Madison.com, case to be prosecuted in South Africa for the contravention of the ECT Act. However in light of the lenient sentences, imposed terms of the ECT Act, should they rather not be tried for the common law offence of fraud? This would not be possible as the ECT Act, falls short of extending jurisdiction for the prosecution of common law offences.

"Hacking" is a novel computer crime, of gaining access to a website without permission.[18] Hacking even though it amounts to unlawful trespassing, does not comply with the statutory offence of Trespass.[19] Hacking is now prohibited in terms of Section 86 (1) of the ECT Act. The internet crime of theft of personal information termed "Identity theft" or "Phishing" does not conform to the traditional common law crime of Theft. The transgression has a greater resemblance to the offence of Fraud as the perpetrator appropriates personal information by means of a fraudulent misrepresentation.[20] "Phishing" is now prohibited in terms in terms of Section 86 (1) of the ECT Act. The ECT Act does not create a Substantive offence termed "Identity Theft".

According to Cassim, the creation of the South African Banking Risk Information Centre (SABRIC), is a positive move to detect and prevent of organised bank related cybercrime.[21] SABRIC could develop to become an educator, to educate the public of the methods and devices used to perpetrate offences

E. Development in international Jurisdictions

South Africa should incorporate policies combating Cybercrime in its national security framework. Instead of creating new strategies, Gercke proposes that ideas from developed countries should be adopted dependent upon capabilities and resources available.[22]

The Netherlands established a Regulatory body which monitors the internet for illicit content[23]. It is recommended that South Africa follows the Dutch and legislate for the creation of a Regulator. Currently South Africa relies on the public to report abuse of cyber networks. Germany established a Federal office for the Security of information Technology

[18] Van der Merwe (n10 above) 63
[19] Snyman *Criminal Law* 551 See: Section 1(1) of the Trespass Act 6 of 1959 criminalises entry into a building or land without permission
[20] Van der Merwe *Information Law* 63
[21] Cassim 2011 *XILV CILSA* 124
[22] Gercke *Understanding Cybercrime* 159
[23] Gercke *Understanding Cybercrime* 162

which was mandated to analyse security risks and advocate measures to combat computer crime[24]. It is proposed that African countries create similar government departments.

The Council of Europe's convention on Cybercrime aims to create co-operation in investigating and prosecuting cybercrime and extradition across multiple jurisdictions.[25] Ratification of the treaty by all African nations is recommended.

In 2014 The African Union adopted a Convention for the protection of cyber security[26] which called for the streamlining of legislation which would solve African problems relating to mutual legal assistance and jurisdiction. It is regrettable that South Africa has not ratified this document, hence the proposals remain ineffective.

F. The effectiveness of the recent developments

Just as Resolution 60 of 177 of the General Assembly of the United Nations acknowledged the vulnerability of countries to cybercrime, the enactment of the ECTA in South Africa has acknowledged this crime. Despite the global nature of the problem, the world response thereto remains fragmented. Cyber criminals hide behind the technicalities such as jurisdiction and problems with definitions, to evade detection and prosecution. In my opinion, for South Africa to fight cybercrime it should ratify the Convention of Europe' on Cybercrime. South Africa should join the global community and provide a co-ordinated response.

South Africa too, is alive to the scourge of cyber crime, and the huge financial implications it has on the economy. However the crimes are only being highlighted by persons suffering financial loss and by the media. Despite this acknowledgement, South Africa is in its infancy in this fight, in comparison to countries such as Germany. South Africa should follow the German response. South African citizens should be educated to enable them to protect themselves from being victims.

Sections 86 and 87 of the ECT Act criminalise cybercrimes. The aforementioned ECT Act, is in line with the recommendations of the Convention of African Union on Cybercrime security and personal data protection. Countries that have not adopted Cyber legislation remain a soft target for cyber criminals. The courts have attempted to compensate for the lack of legislation by finding creative ways to curb the cybercrime, by attempting to extend the common law. The problem in defining cybercrime remains a challenge. The lenient sentences imposed may not serve as a deterrent. To effectively win the war against cyber criminals, I propose the legislature promulgate harsher penalties.

[24] International Review of Penal Law 60 31

[25] Convention of Europe' on Cybercrime adopted in 2001

[26] African Union Convention on cyber Security and Personal data Protection – Adopted on the 23rd Ordinary session of the assembly of the Union , Malabo, 27 June 2014

G. Conclusion

In the final analysis the legal developments in South Africa and internationally can be considered as progressive, however if these developments remain fragmented computer crime will not be addressed effectively. In order to effectively prevent computer crime a multi-disciplinary cooperation between international institutions is necessary.

Bibliography

Articles

1. Cassim F "Addressing the growing spectre of cyber crime in Africa – Evaluating mearsures adopted in South Africa and other regional role players" 2011 CILSA vol XLIV No. 1 March 2011 123-138

2. Mohrenschlager M "Computer crimes and other crimes against information technology in Germany International Review of Penal Law" Volume 64 31

3. Maat Cyber Crime: "A Comparative Law Analysis" 2004 103-108

4. Watney M "Malicious Injury to Property Caused by Computer" TSAR 2005-3 608

Books

1. Gerke M *Undsterstanding Cyber Crime*: *A Guide for Developing Countries* 2nd Ed (ICT 2011)

2. Snyman CR *Criminal Law* 6th Ed (LexisNexis Durban 2014)

3. Van Der Merwe D *et al Information and Communication Technology Law Crimes against information Technology in South Africa (*LexisNexis Durban 2008)

Case Law

1. *S v Howard* Unreported case number 41/258/02 Johannesburg Regional Magistrates Court

2. *S v Ndebele* 2012 1 SACR 245 (GSJ)

3. *S v Van Berg* 1991 1 SACR 104 (T) at 106

Journal Articles

1. Van Der Merwe D "Information technology – A new paradigm shift is needed" 2007 *THRHR* 30

2. D Van der Merwe DP "Computer Crime recent national and International developments" 2003 *THRHR* 30

Websites

1. http://www.un.org/events/11thcongress/

2. http://www.enca.com/life/Cyber-hacking-costly-affair

3. Allen N
http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11640200/Silk-Road-founder-Ross-Ulbricht-sentenced-to-life-in-prison.html (Date of use: 3 September 2015)

Legislation

The Constitution of South Africa Act ,Act 108 of 1996

The Electronic Communications and Transactions Act, Act 25 of 2002

Regulation of Interception of communications Act 70 of 2002

Prevention of Organised Crime Act, Act 38 of 1999

Treaties

The Council of Europe's Treaty on Cybercrime (Budapest 2001)

African Union Convention on Cyber Security and Personal Data Protection (Malabo 2014)