Support for Harmonization of the ICT Policies in Sub-Sahara Africa (HIPSSA)

Sadc Harmonised Legal Cyber Security Framework For Southern Africa

15 – 16 Julyl 2013

Republic of Zimbabwe

Mrs. Revai Sweto - Mukuruba

HIPSSA National Expert

International Telecommunication Union

S Cybercrime on the rise in Zimbabwe: CID (http://www.bulawayo24.com) 24 April 2012

INTRODUCTION

- The Courts in Zimbabwe have played a significant role in the development of computer crime and cybercrime law.
- Currently the Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter referred to as the Code) provides for Computer- related crimes under Chapter VIII of the Act.
- This law is undergoing reform as more traditional offences are now being committed using computers and the internet.
- Since the enactment of the Computer-related crime laws in the Code, they are no specific reported cases which were brought before the higher courts in terms of that law.
- Most cases were dealt with by the lower courts (magistrates courts and these are unreported).
- They are however a few reported related cases which were decided by the higher courts before 2003.
- These cases developed the common law in light of modern challenges in criminal law. They also pointed the need to enact laws on cyber security and cybercrime in particular.

Objectives

- This presentation seeks to highlight;
  - how the common law has affected the development and modification of cybercrime laws in Zimbabwe.
  - how the cybercrime laws or related laws have been interpreted by the courts in Zimbabwe and elsewhere
  - Challenges faced in the interpretation or application of laws related to cybercrime
- Emphasis will be placed on how the draft bill has sought to address some of the challenges presented by common law and to modify the criminal law in as far as it relates to computer crime and cybercrime

Reported Cases: Zimbabwe

Reported cases related to Computer crimes and Cybercrime

In the High Court and Supreme Court of Zimbabwe

Computer related Fraud

Computer – related fraud

S V Chirunga 1998 (2) ZLR 601 (HC)

- The accused was charged with house breaking with intent to steal and theft, but convicted by the Magistrates Court of theft only.
- The facts of the matter were that, the accused was a former employee of a building society.
- He conspired with a cleaner at the society's premises to let him in to the premises after hours, at a time when he had no authority to be there.
- While there he used the society's computer to make fictitious deposits in the accounts of two other persons.
- These persons thereafter withdrew money from their accounts.
- The magistrate acquitted the accused of housebreaking on the grounds that he had been allowed in to the premises by the cleaner, who was lawfully inside.

Computer related Fraud Cont'd

- On review the High Court held that the accused should have been convicted of housebreaking also.
- It was further held that the crime the accused intended to commit was fraud, rather than theft, and he should have been charged with house breaking with intent to commit fraud.
- However there had been theft by false pretences committed when the two account holders withdrew the money.
- The court however noted that it was not necessary to alter the verdict as theft by false pretences was a species of theft.
- In his reasons for judgement the judge noted that in perpetrating the offence of theft by false pretences, the accused gained **illegal access to a computer and fraudulently altered the computer records.**

S V Chirunga (Lessons)

- It is worth noting that, **the computer crimes of unauthorised access, computer related fraud and illegal data interference** were not preferred against the accused because there was no law criminalising such conduct at the time the offence was committed.
- However in 2003 the Code introduced computer related crimes. The offence of unauthorised access is however punishable if committed in aggravating circumstances
- The mere act of unauthorised access without causing injury to the other party is not an offence in itself.
- The draft Bill has modified this provision by criminalising unauthorised access under different circumstances

Defining Computer Data as a Thing

Sv Mutemi 1998 (2) ZLR 290 (HC)

- The accused was convicted of theft from a motor vehicle.
- He had broken in to complainant's car and stole a number of documents.
- The complainant placed a high value on two of the files included in the documents. The accused was convicted based on the intrinsic value of the goods stolen.
- The court held that the general principle of Roman-Dutch law that intangible things could not be stolen had been challenged in modern times. It is quite clear that there are exceptions to that general statement of the law.
- It was held further that Courts in Zimbabwe and elsewhere have dealt with several **cases of computer frauds involving in some cases theft of substantial amounts of money made possible by false credit and debit entries.**
- To suggest in these circumstances that there is no theft is untenable and flies in the face of ordinary logic.
- In 2003, the Code made provision for computer related fraud in aggravating circumstances of unauthorised access (see s 166 of the Act)

Sv Mutemi (Lessons)

- Although the courts in Zimbabwe and else where have made a departure in the common law principle that intangible things can not be stolen.
- (see also the case of **S v Ndebele and another (SS16/2010) [2011] ZAGPJHC 41; 2012 (1) SACR 245 (GSJ)** where I n addressing the question of 'whether or not electricity can be stolen', the Court took a departure from the Roman-Dutch law principle that intangible things cannot be stolen and held that modern day society has already advanced and accepted that there can be theft of this nature)
- It is important to clarify the position in statute for the avoidance of over dependence on judicial interpretation and also to make the law more accessible
- This is in line with the criminal law codification and reform spirit
- The definition of a 'thing' in the draft Bill to include computer data which can be searched and seized is therefore a necessary development in criminal law reform.

Admission of electronic evidence in court

Paradza v Chirwa and others 2005 (2) ZLR 94 (S)

- The applicant applied for a declaratory order that evidence of the telephone conversation the applicant had with Justice Mafios Cheda which the latter tape recorded,
- was obtained in breach of applicant's right to privacy of communications guaranteed under s20 of the 1980 Constitution and
- that admission of such evidence in the proceedings before the Tribunal was likely to violate his right to fair hearing enshrined in S 18(9) of the 1980 Constitution.
- The Court held that in any case it was not the law that evidence obtained as a result of an unlawful interception of a telephone conversation should be excluded from use in court proceedings.
- The admissibility of illegally or improperly obtained evidence is a matter for determination by the court in the exercise of its discretion

Paradza v Chirwa (Lessons)

- The Court relied on s 48 of the Civil Evidence Act [Cap 8:01] which enacted the common law rule on the admissibility of illegally or improperly obtained evidence.
- *(In the South African case of **State v Jacob Sello Selebi Case No: 25/09 South Gauteng High Court (Johannesburg)** the court accepted an intercepted electronic-mail communication as evidence to prove some of the benefits which Agliotti received by reason of his corrupt relationship with the accused.*

The Court did not however address the issue of admissibility or otherwise of the electronic evidence as this was not raised as an issue.)

- The Courts in Zimbabwe have not been faced with the question of admissibility or otherwise of electronic evidence. Arguably the common law rule applied in the Paradza case can be applied to all electronic evidence cases.
- Admissibility of Illegally intercepted communications was addressed through enactment of the Interception of Communications Act [Cap 11:20]. It is therefore necessary to legislate on the admissibility of electronic evidence to avoid it being classified as 'improperly obtained evidence'.
- The admissibility of electronic evidence was accordingly included in the draft Bill.

Illegal Devices

S v Moyo and Anor 2009 910 ZLR 126 (H)

- The accused was charged and convicted by the Magistrates Court with possession of equipment designed or adapted for making infringed copies in contravention of S 59 (1) of the Copyright and Neighbouring Right Act [Cap 26:05].
- On review, the High Court set aside the conviction on the basis that there were flaws in the charges.
- The penalty clause referred to 'specially designed or adopted equipment' the charge sheet and the facts did not allege that the equipment was specifically designed or adapted.
- The court held that mere possession of an ordinary computer capable of burning music CDs and DVDs cannot on its own constitute an offence.
- Modern computers are being manufactured with those basic drivers. It was necessary to allege that the equipment concerned was specifically designed or adapted for making infringing copies.

The Cybercrime Bill makes provision for ***criminalising devices designed or adapted for purposes of committing an offence****. It is therefore necessary to take note of that judgement when prescribing the illegal devices to avoid ambiguity.*

Over broadness (interception of communications)

Law Society of Zimbabwe v Minister of Transport and Communications 2004 (2) ZLR 257 (S)

- The applicant sought a declaratory order to the effect that ss 98 (2) and 103 of the Postal and Telecommunications Act [Cap 12:05] which conferred on the President unfettered powers to direct any telecom licensee or employee of such licensee to intercept any telecommunications if in his opinion it was necessary to do so, in the interests of national security or the maintenance of law and order, were unconstitutional.
- The Court held that the sections were ultra vires s 20 of the 1980 Constitution because they were too wide and vague and did not provide sufficient mechanisms to prevent abuse of the powers conferred therein. The Judge recognised that Section 20 of the Constitution was not absolute in its prescription of interference with communications.
- *The Cybercrime Bill provides for lawful interception of content data after obtaining a court order upon application by law enforcement. The requirement of a court order or warrant to intercept avoids abuse of power by law enforcement agencies.*

Unauthorised Access: Over broadness

***United States v. Auernheimer*, 11-CR-470 (D.N.J.) (SDW),**

Auermer and Spitler were charged were charged with conspiring to access a computer without authorization or to exceed authorized access, and thereby obtain information from AT & T's servers (in violation of the CFAA, punishable as a felony), in furtherance of a New Jersey criminal statute, New Jersey Statutes § 2C:20–31(a). n June 2010,

The brief facts of the case are that;

- Auernheimer] and former co-defendant, Daniel Spitler, created a computer program, designed to exploit AT & T's automated feature which linked iPad 3G users' e-mail addresses to their unique iPad 3G Integrated Circuit Card Identifiers. The Program `was designed to gain access to AT & T's servers.'

- Between June 5, 2010 and June 9, 2010, Auernheimer's and Spitler's Program gained access to AT & T's servers and obtained approximately 120,000 ICC–ID/e–mail address pairings from iPad 3G customers, including thousands of customers in New Jersey. Subsequently, Auernheimer and Spitler disclosed the obtained information to Gawker, an Internet magazine, and sent e-mails to members of various news organizations .

Auernheimer Case Cont'd

- Auernheimer was found guilty of unauthorised access (and other counts) and sentenced to 41 months to pay restitution in the amount of $73,167.00
- *Auernheimer has appealed against his conviction in July this year and his case is still pending*
- The decision in the ***Auernheimer*****,** case has been criticised on the grounds that the accessed information was not protected and the accused were punished for mere access of public information without infringing any security measures
- The Computer Fraud and Abuse Act has been criticised for failing to define what constitutes unauthorized access to a protected computer. (whether unauthorised access occurs when the owner of the computer system says so).
- It has been argued that to avoid abuse of prosecution powers, cases of unauthorised access should be limited to illegal hacking only
- The USA Government has been criticised for interpreting the CFAA too broadly

How the Draft Bill has sought to address some of the problems in the Auermer Case

- The draft Bill has to some extent addressed the problems of over broadness in unauthorised access cases in that;
- the draft Bill has distinguished cases of
  - ❖ mere unauthorised access,
  - ❖ unauthorised access through infringement of security measures and
  - ❖ unauthorised access in furtherance of the attempted commission or commission of an offence or in aggravating circumstances
- The distinction is in line with the provisions in the Code (*the code distinguishes mere unauthorised access and unauthorised access in aggravating circumstances and provides for different levels of penalties)*
- The distinction is necessary as it provides for prosecution discretion in preferring charges and also in sentencing
- This avoids unfair or broad application of the law in different circumstances.

Conclusion

- Judicial interpretations of the common law in relation to computer crime and cybercrime offences have contributed immensely in the development of the computer crime and cybercrime laws
- The common law has also helped to point out gapes in the application of the criminal law to sophisticated modern offences arising from technological developments.
- Zimbabwe (in Chapter VIII of the Code) has a cybercrime framework aimed at addressing the prevention of illegal hacking of computers in furtherance of the commission of other serious offences.
- It does not however cover other computer crimes such as illegal system interference, spam , illegal devices etc.
- The draft bill provides for the modification of the Code in keeping up with the spirit of harmonisation of the national laws with the SADC Model Laws and international best practices.

Contacts

Thank you for your attention

For more information: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/index.html

Sandro Bazzanella
ITU-EC *Project Manager*

sandro.bazzanella@itu.int

Phone: +41 22 730 6765
Fax: +41 22 730 5484

Ida Jallow
HIPSSA Senior Project Coordinator

Ida.jallow@itu.int

Phone: +251 11 551 4977
Fax: +251 11 551 7299

ITU-EC Project - Harmonization of ICT Policies in ACP countries

International Telecommunication Union
Headquarters
Place des Nations
CH-1211 Geneva 20
Switzerland

International Telecommunication Union
Regional Office for Africa
P.O. Box 60 005
Addis Ababa
Ethiopia