CHAPTER 12

JURISDICTION

12.1 INTRODUCTION

If one looks at a traditional map of the world one can easily distinguish between the various continents and countries since their boundaries are clearly stipulated. However, cyberspace does not adhere to these traditional boundaries. The Internet is a worldwide network compromising of computer networks and is also known as the information superhighway.[1] A person in South Africa can access websites located all over the world. A website may comprise of information obtained from various countries and one may not even be in a position to realise where the website is actually situated.

Computers and systems all over the world are linked through information networks and a person located in one country can easily commit a cyber crime in another country without even being physically present in the country where the crime was committed. Traditional telephone systems are outdated and one can gain access to networks through cellular phones and even satellite. Wireless technology will make it easier for a cyber criminal to commit crime of a borderless nature. One therefore does not need to be in a specific country at all. It is perceivable that one can commit a cyber crime whilst on a private yacht in the middle of an ocean.

---

[1] See in general Reinhardt Buys *The Internet: an overview* in Buys(ed) *Cyberlaw @ SA* (2000) 11-36.

Jurisdiction in respect of cyber crime is a complicated issue. For example a person situated in the United States creates a website and posts child pornography on this website. Since this website is located on the Internet it can be accessed by a person situated in South Africa. The perpetrator in the United States in essence distributes child pornography in South Africa through this Internet website. Recently in the United Kingdom jurisdiction in respect of the Internet was considered and it proved to be rather complicated.[2]

12.2 INTERNATIONAL RESPONSE BY THE COUNCIL OF EUROPE

The Council of Europe's Convention on Cybercrime suggested certain guidelines in relation to jurisdiction in respect of cyber crimes.[3] A country has jurisdiction if the cyber crime was committed:

1. in its territory;
2. on board a ship flying the flag of the country;
3. on board an aircraft registered under the laws of the country;
4. by one of the countries nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.[4]

---

[2] Dawn Osborne *Jurisdiction on the Internet – not such a barrel of laughs for Euromarket!* (2000) 11 Computers & Law 26-27. Also see Michael Hirst *Cyberobscenity and the Ambit of English Criminal Law* (2002) Computers & Law Vol. 13 Issue 2 25 *et seq*.

[3] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest 2001 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[4] Article 22 of the Convention on Cybercrime

12.3 SOUTH AFRICAN POSITION

The general rule is that when a crime was committed outside the borders of the Republic of South Africa, a South African court will not have jurisdiction to adjudicate the case.[5] The Electronic Communications and Transactions Act provides for issues of jurisdiction in accordance with the provisions of the Convention on Cybercrime. Section 90 of the Act states:

> "A court in the Republic trying an offence in terms of this Act has jurisdiction where-
>
> a. the offence was committed in the Republic;
> b. any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;
> c. the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or
> d. the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed."

Section 90 is far more comprehensive than the guidelines of the Convention on Cybercrime. The inclusion of subsection (b) is useful since it provides for jurisdiction in instances where only certain elements of the cyber offence were committed in South Africa. Viruses that are introduced into computer networks overseas may have consequences or affect networks and computers in our country. Subsection (b) provides for

---

[5] See Adv B Gordon *Cyberspace and physical borders – The Internet's ultimate challenge* (July 2002) Servamus 32 – 33.

jurisdiction in instances where *any result of the offence has had an effect in the Republic*. If a hacker located in the United States accesses a computer network in South Africa and causes damage to the South African network, a South African court will have jurisdiction in respect of the crime.

It is a real possibility that more than one country may establish jurisdiction in respect of a cyber crime. The problem that arises is in which country should the perpetrator be prosecuted. The Convention on Cybercrime states that when more than one signatory country claims jurisdiction in respect of an offence the countries should consult to determine the most appropriate jurisdiction for a prosecution.[6] The country in which most of the elements of the crime were committed or the country that was affected the most by the crime could be decisive. The location of witnesses could also be an important factor to take into account.

The wording of subsection (c) may yet prove to be problematic to interpret. Does this subsection mean that a South African court will have jurisdiction to try a case where *all* the elements of the crime had been committed *beyond* it's borders, *no effect* is felt in South Africa and the provisions of subsection (d) are not applicable, merely because the offence was committed by a South African citizen or one of the other categories of persons mentioned in subsection (c)? According to the Convention on Cybercrime this aspect is based on the principle of nationality and provides that nationals of a State are "obliged to comply

[6] Section 3 Article 22(5) of the Convention on Cybercrime.

with the domestic law even when they are outside its territory".[7] The Convention sets the additional requirements that the conduct must also be an offence under the law of the State in which it was committed *or* the conduct has taken place outside the territorial jurisdiction of *any* state. Section 90(c) of the Electronic Communications and Transactions Act in this regard is much wider and does not contain these additional requirements. It seems that a South African court will have jurisdiction if a South African National commits a cyber crime abroad based solely on the South African connection of the perpetrator. It is submitted that this subsection in the Act is very broad and could prove to be highly impractical. It is suggested that in an instance where no country has established territorial jurisdiction in respect of an offence, the nationality of the perpetrator should play a decisive role in deciding where he should be prosecuted and it is submitted that this is what the Convention had in mind with this provision.

The Act refers to *a court in South Africa* and will include district courts, regional courts as well as the High Court of South Africa. Section 90(1) of the Magistrates' Courts Act[8] states that "any person charged with any offence committed within any district or regional division may be tried by the court of that district or of that regional division". The provisions in section 90(d) of the Electronic Communications and Transactions Act may prove to be problematic in view of the jurisdictional provisions contained in the Magistrates' Courts Act. In terms of the Magistrates' Courts Act a court has jurisdiction if the offence has been committed within its territorial borders and this is contradictory to the provisions of

[7] Paragraph 236 of the Explanatory Report to the Convention on Cybercrime (ETS No. 185).

[8] Act 32 of 1944.

section 90(d) of the Electronic Communications and Transactions Act that provides for jurisdiction in terms of nationality and not because the offence has been committed within its territorial borders. Another aspect that needs to be considered is if a cyber offence is committed beyond our borders and the South African offender is prosecuted in South Africa, in which regional court or district court must the offence be prosecuted.

If one has regard to the maximum penalty provided for by the Act, a district court would in all probability adjudicate these new types of offences. A regional court will probably hear cases of a more serious nature or where considerable damage was caused. In practice a regional court will hear cases of fraud and theft involving amounts exceeding R 60 000. Computer-related theft and fraud involving smaller amounts would be adjudicated by a district court.

Assessors may be appointed to sit with a Judge or Magistrate during a trial. An assessor is a person who, in the opinion of the presiding Judge, has experience in the administration of justice or skill in any matter that may be considered at the trial.[9] Judges and Magistrates are often not computer literate and might find it difficult to follow evidence of a highly technical nature. It is fortunate that a Judge or a Magistrate may appoint an assessor, who is an expert in the field of computers and information technology, to assist in the just adjudication of the matter.

[9] Section 145(1)(b) of Act 51 of 1977.