CHAPTER 16

SIGNING OFF

Information technology and computers are valuable tools in the detection, investigation and proof of crime. The advent of computers, however, has also resulted in new and technologically advanced methods to commit crime. New types of crime have surfaced and existing crimes are now also perpetrated through means of sophisticated technology. Initially computer crime focused on computers, but with the advent of information networks and the Internet, the focus has moved to information technology and data. Cyber crime therefore encompasses all those illegal activities where computers and data are the target of the crime and those known illegal activities that are now actively committed through computers and information technology. Certain common law offences and statutory crimes exist in a physical and tangible world and cannot be forced to operate in an intangible and abstract world of information networks and data. It is apparent, as in many countries, that intervention by the legislator was necessary. Internationally many countries enacted legislation to address cyber crime. The problem in relation to the criminalisation of these types of offences has very effectively been dealt with by the enactment of the Electronic Communications and Transactions Act 25 of 2002. The Act has changed our law dramatically in respect of cyber crimes and related procedural and evidentiary matters and the *lacunae* that existed in respect of cyber and information technology crime were eradicated.

The criminalisation of hacking offences (unauthorised access) was long overdue and the legislator succeeded in enacting plain language provisions that will assist in the prosecution of these matters. The past decade has shown us the frequent occurrence and destructiveness of viruses, worms and other forms of rogue computer codes. The criminalisation of modification of data was therefore necessary in view of the recent spate of viruses and other forms of malicious code. The criminalisation of the possession and distribution of hardware devices and software programs used in the commission of cyber crimes is a welcome addition to our law especially in so far as they facilitate the commission of cyber crimes. The denial of service to lawful users of computers and computer systems as a result of these offences are also sanctioned with a criminal penalty.

The legislator can however be criticised in two respects. The first aspect is directed at the penalty provisions provided for by the Act. The penalty of a fine or a maximum of 12 months imprisonment in respect of unauthorised modification offences such as viruses is in my view far too lenient. These malicious programs may have disastrous consequences and the impression is created that these types of offences are not viewed in a serious light. The second point of criticism relates to the fact that key concepts such as *access* and *unauthorised* were not defined by the Act. However, these concepts will certainly be interpreted in the light of the objectives of the Act.

Unauthorised interception offences are now governed by the Electronic Communications and Transactions Act as well as the new Regulation of Interception of Communications and Provision of Communication-

Related Information Act 70 of 2002. Online child pornography is sufficiently criminalised in the Films and Publications Act 65 of 1996.

Section 87(2) of the Electronic Communications and Transactions Act in relation to computer-related fraud ends the debate in respect of the questions whether a misrepresentation can be made to a computer and whether a computer can be deceived. The provisions in respect of *spamming* are of great value to those who are pestered on a daily basis with this form of junk e-mail. The computer-related extortion provision is perhaps unnecessary (since the common law offence of extortion is wide enough to encompass computer-related extortion), but is advantageous since extortion is defined in a cyber context.

It is clear that our legislator is silent on the issue of theft of information and it may be argued that they have decided to leave this aspect to the judiciary. A proper analysis of the law, especially in relation to the theft of credit, leads to the conclusion that theft of incorporeal items is recognised in our law without however expressly stating it. The courts may be hesitant to develop the law in this regard and development may take time. There may still be problematic areas such as the mere copying of data under certain circumstances that is not covered by the offence of theft, the Electronic Communications and Transactions Act or copyright protection. It is submitted that the legislator should intervene with a statutory provision in order to criminalise unauthorised use and unauthorised copying offences.

The development of the provisions of the Electronic Communications and Transactions Act and related cyber crimes will take time and specific requirements and limitations will be developed in due course through the

judiciary. In order for the law to develop in this regard cases must be detected and reported. Effective investigation and prosecution of these crimes by skilled investigators and prosecutors will assist in this process.

A cyber policing unit in the form of cyber inspectors may assist a great deal in the detection and investigation of cyber crime. Of utmost importance is that encryption and electronic signatures have been afforded legal status. The regulation of encryption products and service providers will protect consumers. The provisions in respect of the admissibility of data messages will promote legal certainty in this field.

Finally it is suggested that, when it is necessary to use the provisions of this Act, everybody involved in the investigation and prosecution of these crimes do not flinch from that which is unknown but that they do so with confidence and conviction. This in turn will promote positive judgements by judicial officers and will assist in the effective combating and prevention of this global phenomenon.