9 Slotbeskouing

Om aan 'n vakbond die reg te verleen om te mag assosieer en organisatoriese regte uit te oefen maar dit die mees basiese vakbondreg te ontsê, naamlik om effektief kollektief te mag te beding, is so goed as om vir 'n persoon motor sonder 'n enjin te gee – hy sal die voertuig slegs kan gebruik as daar telkens direkte daadwerklike eksterne "ingryping" plaasvind. Verder, om die reg op kollektiewe bedinging te erken maar te ontken dat daar 'n meegaande verpligting om te beding, bestaan maar dat die reg nietemin erken en verskans word deur die uitoefening van stakingsregte of verpligte arbitrasie, is arbeidsregtelik nie praktries, sinvol en in belang van harmonieuse arbeidsverhoudinge nie. Voorstanders van die standpunt dat die Grondwet slegs vir 'n vryheid, en nie 'n reg van kollektiewe bedinging nie, voorsiening maak, is self bereid om toe te gee dat die skeidslyn tussen die twee gevalle delikaat is en dat daar moontlik ruimte en meriete vir 'n teenoorgestelde sienswyse is.

Daar moet voortdurend onderskei word tussen die fundamentele reg op kollektiewe bedinging, aan die een kant, en die meganismes, partye, onderwerpe van bedinging en uitkomste van bedinging, aan die ander kant, wat totaal vrywillig is. Die onderhawige reg is ook nie absoluut nie en daarom moet 'n party telkens aan bepaalde vereistes voldoen soos neergelê in die Wet op Arbeidsverhoudinge van 1995. Indien te doen gekry word met uitsonderlike gevalle soos lede van die Weermag, kan die fundamentele reg ingevolge artikel 36 van die Grondwet aan sinvolle beperkings onderhewig gestel word sonder om die werking en toepassing daarvan totaal te neutraliseer of kragteloos te maak.

As kollektiewe bedinging dan in die verlede die wyse was waarop arbeidswanverhoudinge en -dispute besweer is, as kollektiewe bedinging die hartslag van gesonde arbeidsverhoudinge was en die hoeksteen daarvan gevorm het (*Buffelsfontein GMC*), is dit onduidelik en onverstaanbaar waarom daar soveel weerstandigheid teen die afdwingbaarheid van hierdie internasionaal erkende fundamentele reg bestaan. Miskien is die volgende versugting van regter Sachs in *SA National Defence Union v Minister of Defence* 1999 20 *ILJ* 2265 (KH) 2285G–H *in casu* tog *mutatis mutandis* van toepassing:

> "Nor, conversely, do I feel it appropriate in this matter to grapple with the possible implications of what would at first sight seem to be the relative ease with which some or all of these rights could be subjected to extensive limitation, thereby suggesting that they could be imbued at their core with a fragility and relativism out of keeping with their hard-won, resilient and firmly entrenched character."

FANIE VAN JAARSVELD
Universiteit van Pretoria

INFORMATION TECHNOLOGY CRIME – A NEW PARADIGM IN SOUTH AFRICA

1 Trying to define "computer crime"

During the seven years that have elapsed since I released my work entitled *Computers and the law* (2000) on an unsuspecting South African public, the basic

concept of "computer crime" or "IT crime" does not seem to have gained much in clarity. In that work I settled for the following definition of "computer crime":

> "Computer crime covers all sets of circumstances where electronic data processing forms the means for the commission and/or the object of the offence or represents the basis for the suspicion that an offence has been committed" (188).

In the same chapter, I also took trouble to cite my later court protagonist during the long-lasting "Boeremag" trial, which is still continuing as I write the present note. This was Superintendent Grobler, the police expert witness who had confiscated and examined both IT and GPS equipment found in the suspects' possession. Grobler is of the opinion that:

> "Computer crime is any illegal act which involves a computer system whether the computer is an object of a crime, an instrument used to commit a crime or a repository for evidence related to a crime."

Even though the relevant IT equipment in this particular trial proved to be a bountiful *repository* of evidence possibly relevant to the crimes charged, the State's case was very much based on the fact that computer systems (as well as GPS systems) were also *instruments* used to commit a crime. Although one has sympathy with Superintendent Grobler's viewpoint that a computer repository for evidence might turn a specific criminal case into one of "computer crime", almost all statements in police dockets are being typed on computers these days and this might render the final part of his definition too wide. Come to think of it, even the final part of my own definition, which includes data processing as the "basis for suspicion that an offence has been committed", might also be too broad.

In other words, we are looking for a better definition for "computer crime", or perhaps with a bit more vision, for a more fundamental re-think of the entire concepts of wrongdoing and information technology and the interface between the two.

When exploring the work of my publishing protagonist, the author and lawyer Reinhardt Buys who edited and wrote *Cyberlaw@SA* (2004), one finds yet another definition of "computer crime" (320). This work makes use of an overseas definition by Casey that distinguishes between cyber crime and computer crime. The former is "any crime that involves computers and networks, including crimes that do not rely heavily on computers" and the latter "a special type of cyber crime", which crimes are specifically defined in recent internationally relevant Acts such as the Computer Fraud and Abuse Act of the United States and the Computer Abuse Act of the United Kingdom. I am afraid that the same criticism of being too wide could be levelled against the latter two definitions.

Professor Jonathan Burchell, my academic colleague, has also tried his hand at an evaluation of "computer crime" during his inaugural lecture as professor of criminal law at the University of Cape Town on 24 April 2002 (published 2002 *SALJ* 579ff). He distinguishes (585) between using a computer as an object (or victim) and using a computer as an instrument to commit a crime, and argues that the latter type of activity might already be covered adequately by existing common-law crimes. Even when defining new crimes to protect a computer as an object, he argues for restraint, and appeals strongly that "any legislative intervention must be meticulously defined and costed and personnel who will be called on to implement it, trained to do so". This is an admirable sentiment, but might be better accomplished by a deeper analysis of the real legal interests involved in a superficial term such as "computer crime".

2 What are the true legal interests underlying these definitions?

From the previous section it has become clear that "the infernal machine" (the computer or "hardware" itself) still forms an important part of most lawyers' thinking as far as "computer crime" is concerned. As the attentive reader might gather from the title of the present note, I have undergone my own Damascus conversion in this regard, seeing that the present note attempts to deal not with computer crime, but with "information technology crime." To try and put my own insights into a nutshell: the "computer" itself is a mere container, manipulator or even just a shell – the good stuff (information or data) is inside.

In an earlier article "Computer Crime – recent national and international development" 2003 THRHR 30ff, I tried to indicate how the concept of "valuables" has changed over the centuries. One model of thought that might assist readers in this regard is that of Toffler, author of *The third wave* (1981). During three separate era's of human development three different value systems have held sway over our affections, our market-related activities and our motivation and methods to "become rich". During the so-called "First Wave" (or Agricultural Revolution), *land* was the trump card. In fact, if you held land, it not only gave you a fancy title (such as "the Duke of Rochester" or "the Earl of Salisbury"), but also the right to decide over peoples' very lives (provided that they lived on your land). During the "Second Wave" (or Industrial Revolution) *capital* sums of money (and later on, an organised *labour* force) were the trump cards for financial gain. The "Third Wave" is characterised by activities which Toffler calls "tele-commuting" and "the electronic cottage" but these all converge in an over-arching idea that because *information* (the latest "valuable") travels easily, it might no longer be necessary for information workers to travel to a centralised place of work. We have recently started to see work being outsourced by the parent company (say, in the United States or Europe) to a new generation of IT workers (say in India or China) because IT workers in the latter countries are satisfied with a lower hourly rate.

Obviously this development has profound implications for world-wide employment and labour relations, but the implications for legal systems world-wide seem equally radical. Suddenly questions such as international jurisdiction as well as the "portability" of labour contracts between different continents are starting to assume proportions which they have never had during the industrial "Second Wave". In addition, age-old areas of the law, such as the law of things, are now starting to have to cope with slippery (but valuable) intangibles called "data", "information" and "knowledge", which nothing in the past has prepared them for. Nonetheless, the scope of the present note is simply to look at IT crime in greater detail and particularly at the legal interests involved, with a modicum of attention to related aspects such as criminal procedure, jurisdiction and proactive IT security.

The procedure followed by the present note is to put forward the author's view of the true legal interests which stand to be protected by South Africa's provisions against IT crime, and then to test these interests against the actual provisions. A second and more speculative step will be to make an educated guess as to the possible success and effectiveness of such provisions in addressing (or at least containing) IT crime in South Africa.

In *Computers and the law* xviii, I used a distinction originally made by Twine at a conference entitled "Knowledge Management – overcoming the information overload" (held at Kyalami, Gauteng on the 5 August 1998). This distinction

grades the following concepts in an ascending order of information value: "data", "information", "knowledge" and "wisdom". The concept of "intelligence" works as a catalyst on the other four, transforming (objective) data to (subjective) information, information to knowledge and knowledge to wisdom. Twine then argues (convincingly, I think) that among the four factors of production resources (namely land, capital, labour and entrepreneurship) only the latter actually possesses the intelligence to "process" one of the lower factors to a higher, next level: "He who owns the intelligence is king!"

Taking this argument to its ultimate consequence would mean that "data" is the real gold ore which needs to be processed intelligently in order to lead to higher forms of information value. For this reason the South African criminal law system urgently needed to formulate crimes which would protect the integrity and inviolability of data, particularly because our criminal law has historically focused on protecting tangible assets and money. Any criminal law system which fails to adequately protect one of the most valuable commercial resources, will ultimately fail in its purpose.

3 The new "IT-crimes" created by statute

In 1998 the South African Law Commission published an issue paper entitled *Computer-related crime: preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects* (SALC Project 108 – Issue paper published on 6 October 1998). This title highlights three important vulnerabilities of information technology that the traditional South African criminal law probably did not address, or did not address adequately.

Unauthorised access to any database (whether stored on "computer" or other backup media) is the equivalent of common-law housebreaking, especially because of the possible value of the data stored on the database. When asked why he robbed banks, the (in)famous American bank robber Jesse James reportedly replied "because that's where the money is!" Today, databases are "where the money is" and the legal system cannot leave such valuables unprotected.

The other two actions that the issue paper hoped to declare "off limits", were the unauthorised modification of data and software. These actions should be roughly equivalent to our common-law crime of malicious injury to property, except for the fact that the "property" now consists of valuable computer data or the software applications that marshal and arrange such computer data.

The various inputs received from commentators on the issue paper led to a discussion paper with the same title (SALC Project 108 – Discussion paper published on 2 July 2001). The discussion paper also suggested draft legislation that would address most of the legal issues that had been discussed up to that point. However, these developments were then caught up by a new wind blowing from the South African Department of Communications (DOC). The DOC had been inspired by world-wide developments in the area of electronic commerce and wanted South African legislation to be in a fit state to control and encourage electronic commerce locally. In the end, the energetic intervention by the DOC led to a speedy implementation of the Electronic Communications and Transactions Act (ECT Act) 25 of 2002 that covers a number of topics dealing with the interface between the law and electronic commerce. For purposes of this note, Chapter XIII of the ECT Act is of specific interest, seeing that it specifically relates to "cyber crime". Even though the title, standing by itself, might sound

like just another species of "computer crime", a closer scrutiny of the new statutory crimes themselves make it quite clear that data is the real legal interest that stands to be protected.

Section 86(1) of the ECT Act criminalises any unauthorised "access to, interception of, or interference with data", thus adding "interception of" and "interference with" to the actions of unlawful access and modification which the SALC had thought to prohibit *in connection with* data. Section 86(2) specifically prohibits any unlawful modification of data in the shape of "interference with data" which would cause such data to be "modified, destroyed or erased or otherwise rendered ineffective". This section would cover the creation and distribution of computer "virus" programmes (see below), provided that, together with the other elements of a crime, the necessary causal link and *mens rea* could be proved. The latter would probably often take the form of a kind of *dolus eventualis* ("I foresee a reasonable possibility that my programme will interfere with someone else's data, and I simply do not care"), together with a kind of *dolus generalis* ("I foresee a reasonable possibility that my programme will interfere with someone else's data, and I simply do not care whose data that is").

Section 86(3)–(4) of the Act deals with the "tools of the trade" for carrying on some of the activities discussed in the present paragraph. The dealing in, or utilisation of such devices are criminally prohibited. Section 86(5) deals with a so-called "denial of service" attack. This means that anyone who performs electronic actions that slow down, or stop a lawful user's access to IT services, is committing an offence.

Section 87 of the ECT Act creates statutory and data-related forms of extortion, fraud and forgery, but this would probably fall under what Professor Burchell calls "using a computer as an instrument to commit a crime" and one would need to answer his argument that the latter type of activity might already be covered adequately by existing common-law crimes. An attempt will now be made to do exactly that, by taking a look at and describing some of the interesting (though perverted) new criminal schemes which threaten either the integrity of data (s 86 etc) or the hard-earned electronically-stored finances of victims (s 87 etc), and then judging whether the new arsenal of "cyber crimes" are adequate to meet the new threat.

4 New forms of criminal behaviour targeting data and/or electronically stored finances and the response of the law

4 1 Hackers

These individuals are the electronic equivalent of our common-law housebreaking criminals who attempt to break into physical premises for whatever nefarious purpose. Ironically, "a good hack" used to be a term of honour and skill bestowed upon skilful (and lawful) programmers, but nowadays it is mostly used to describe an uninvited electronic guest. It is also interesting to note that companies who have updated their digital defences sometimes employ the services of an "ethical hacker" who undertakes to test these defences and inform the company whether its "firewall" (a series of electronic defences and passwords) may be considered hacker-proof.

Two ways to test these defences are by means of "port scanning" and "ping flooding" (see Ebersöhn "Internet law: Port scanning and ping flooding – a legal perspective" 2003 *THRHR* 563). Port scanning is achieved by simply sending a

probe to scan which computer ports on a computer or network are vulnerable to attack, and ping flooding consists of flooding a specific computer with "ping" signals (normally a harmless electronic signal inviting a response from the computer being "pinged") so as to cripple the receiving computer. Ebersöhn tests these two activities against the wording of section 86 of the ECT Act and finds that "ping flooding" would quite probably fall within the scope of section 86(5) because it indirectly interferes with data by causing the entire system, including the data, to become ineffective. On the other hand, for port scanning to fall clearly within the section, Ebersöhn recommends that the wording of section 86(5) be amended from committing "an act described in this section" to committing "an act with intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users". This seems to me, as the author of section 86, to be a valid comment, and I would recommend that such an amendment be made to the section.

There does not seem to be any problem in utilising section 86(1) of the ECT Act to prosecute ordinary hackers sourced in South Africa, and a number of successful prosecutions have been undertaken. The only bone of contention seems to be a slightly low maximum penalty of 12 months imprisonment for an ordinary hacker, which many of the enforcement authorities consider to be inadequate.

Many hack-attacks are, however, sourced from overseas, which brings about a number of jurisdictional and procedural problems. South Africa has taken the first steps towards addressing these problems by becoming a signatory to the European Community's Convention against Cybercrime (ETS No 185, Council of Europe, Budapest 2001). The ECT Act probably goes some way towards addressing South Africa's substantive obligations in terms of the treaty, but a number of procedural and administrative measures still remain outstanding (eg, a 24-hour per day, seven days a week contact centre for sending and receiving requests by law-enforcement authorities in the treaty countries).

It is important to remember that the computer hardware, by itself, is not so much the victim of these attacks, as is the data, which loses value, integrity and/or exclusivity because of the intrusion(s).

4 2 Virus programmes (including "root-kits")

These programmes were originally termed "virus" programmes because their (digital and electronic) means of propagation are analogous to the (physical and biological) means followed by a cold or flu virus. In the same way that one may build up one's physical defence systems by taking a course of Vitamin C, one may install the latest anti-virus programme in order to prevent and forestall an "infected" computer, particularly when one has to connect to other computers by means of the Internet or Local Area Networks (LANS) on a regular basis.

A "virus" is usually an active computer programme that interacts with other lawful programmes, slowing down the working of the latter or rendering their performance unreliable. It does so by attaching itself to a file or to the boot sector of a diskette, or other removable media, or (by means of the Internet or a local network) to the hard disk of the affected computer itself. A "zoo virus" (see www.westcoastlabs.org for information on this and some of the next programmes) is a virus which is not causing any problems at present, either because it was written for outdated software, or was never released onto the Internet (often because it was only used for laboratory testing). However once a virus

"gets out in the wild" it may get onto the "wildlist", which is a monthly list of potentially damaging viruses produced every month by volunteers. To qualify, the virus needs to have been seen by the customers of at least two or more reporters who are based in at least two or more countries.

A "key-logger" is a simple programme that makes a note of one's keystrokes and purveys this information to its creator as soon as one goes on-line on the Internet or logs onto one's network. In this way, valuable access codes and other strategic information may fall into the hands of outsiders. The key-logger is a simple form of more sophisticated "spyware" which might have been placed in one's computer to convey more sophisticated information to its outside masters.

A variation on this theme of viruses is a "worm", which simply keeps replicating itself without interacting with, or attaching itself to, other programmes. This gradually slows down the working of one's computer because the existing memory space is slowly but surely consumed by the worm, until lawful programmes have virtually no memory space left within which to operate.

The most recent (and sinister) variation on the virus theme, is a so-called "root-kit" (see November 2006 *PC Advisor* 100ff for an article entitled "Protect your PC", which is also the source of some of the following information). The root-kit consists of an entire suite of programmes, surreptitiously downloaded onto the victims' computer by the perpetrator. The actual act of downloading is usually done by means of a "downloader", which is a programme which "gets in first" onto the affected computer and which then, when activated, downloads files onto such computer without the knowledge and consent of the lawful user. This all happens by means of a "back-door" which is a way of getting access to a system by exploiting a vulnerability in the system – the lawful owner has "left the backdoor open"!

By means of the root-kit, the intruder may then carry out his nefarious schemes upon the afflicted computer, while preserving the illusion of normality in the eyes of the lawful owner. Root kits thus allow viruses, worms and "bots" to "hide in plain sight" on one's computer, while subverting most of the computer's resources to the whim of the uninvited visitor. The "bot" is short for "robot", and is supposed to convey the "bot" programme's slavish adherence to the commands of its outside master. Part of the outside perpetrator's goal is to add one's own personal computer to his (or her) network of "bots", or "bot-net". The perpetrator may then use the victim's computer as a "proxy" to conduct attacks or send spam to other potential victims. He (or she) may even announce news of the "exploit" on the Internet so as to enable other potential evil-doers to also abuse the poor computer!

A collective term for software that performs the damaging actions described above, is "malware", short for "malicious software".

Fortunately, section 86(2) of the ECT Act has been framed specifically to take care of the above activities and is also framed widely enough so as to bring most, if not all, of these activities within the four corners of the statute. The section provides as follows:

> "A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence."

There seems to be little doubt that planting any malware, whether in the shape of a virus, a key-logger, spyware, a "bot" or an entire "root-kit", onto a computer or

network or database would sufficiently interfere with the data of the owner to create a contravention of section 86(2). There seems to be good grounds to assume that such interaction would "cause such data to be modified, destroyed or otherwise rendered ineffective".

A twinge of doubt might remain with regard to the activities of the "worm" that simply consumes user memory without really actively interacting with any of the lawful user programmes. I am fairly sure, however, that most courts would give a sufficiently liberal interpretation to section 86(2) so that the section might also include the restricted access to one's lawful data under the terms "otherwise rendered ineffective". A strong analogy exists with the common-law crime of malicious injury to property, where even restricted access, or access which is dependent on some prior time-consuming activities, has been seen to constitute "injury" or "damage" to such property even though such property may (after some trouble and/ or expense) be restored to "as good as new".

4 3 "DNS server" attacks

Part of one's valuable real estate on the Internet often consists of a so-called domain name. This is the distinguishing word (or words) by which one's website is known on the Internet, and is often a valuable piece of intellectual property – almost a combination of a trade mark and a trade name. The fact that a full domain name leaves scope for national diversification does make the scheme a little bit more flexible. Thus "triumph.co.za" represents South African packing material, "triumph.co.uk" represents a famous British motorcycle and "triumph.com", the mother of them all, represents ladies' brassieres. Personally I have registered "profdana.co.za" as a type of electronic calling card for use on the Internet, electronic mail and (recently) on the short messages system (SMS) of mobile commerce.

The threat which DNS server attacks pose, usually centralises on the "always-on" computer server presented by your ISP (Internet Service Provider), which has to stand waiting idly for anyone interested to do a search for, or a visit to, a specific domain hosted by that particular server. These DNS servers translate website addresses into the numerical IP addresses that personal computers need to find each other on the Internet. The server cache may be "poisoned" in order to spread malicious software or even to gain control over the entire DNS server.

Even though the ECT Act provides specific protection for the intellectual property contained in the domain name itself (the entire Ch X of the Act (ss 59–69) is devoted to this purpose), any DNS server-attacks would probably be open to criminal charges in terms of section 86(2) above, as constituting "interference with data". Not only that, but they might very well also constitute a contravention of section 86(4), which criminalises the act of using a device or computer programme in order to overcome security measures designed to protect computer data, or access thereto. Finally, a state prosecutor may also consider charges in terms of section 86(5) which criminalises any act described in section 86, committed "with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, or service to legitimate users". Surely most DNS server attacks would constitute at least a partial denial of service to legitimate users?

4 4 "Phishing" attacks

The action of "phishing" basically boils down to a website that impersonates that of your bank or an on-line auction or shopping site usually patronised by yourself

when on-line on the Internet. It is, however, a false site which exists merely to trick you into revealing personal details which it may use for later access to your sites or, even worse, which information it may sell to the highest bidder. The false site is therefore "fishing" (or "phishing") for information for illegal use later on. Users should be very careful of unexpected e-mail messages purporting to originate from one's bank or financial institution, requesting one to "click on a link to verify your account details". Again, it is interesting that data itself is seen as a worthwhile object of attack, with the financial reward only coming indirectly.

A recent innovation by the phisher community is a technique called "smart redirection", where a virus programme may be sitting on one's computer, having been pre-programmed to be on the lookout for the addresses of certain banks. Upon this address being typed in by the lawful customer, the programme "re-directs" the user to a false "banking" site where even more personal information might be extracted by the phishing programme. According to a recent quote in the computer press, "not only can phishers sell the credit left on your card, but they can sell your identity, too" (see November 2006 *PC Advisor* 104). This activity has come be known as "identity theft", although it does not fit well with the common-law definition of theft.

Because of the misrepresentation that takes place by means of phishing and redirection, these types of activities could quite probably be charged as a form of common-law fraud in a criminal court, but a contravention of section 87(2) of the ECT Act would probably make a good alternative charge. That subsection provides as follows:

> "A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence."

The unlawful access to, and interference with, proprietary data by the phisher would take care of the first requirement of the quoted subsection, whereas the rest of the section is tailor-made to cover phishing activities.

4 5 Spam

This is a four-letter word, originating from a BBC-programme on a character entitled "Monty Python", which means (lots of) unwanted electronic communications, either by means of the Internet or by means of the cellular network. After receiving some kind of service, one is often persuaded to fill out an "evaluation form", often with the promise of some vague and nebulous reward. One of the fields usually consists of one's e-mail address, or cell phone number, and these are then used afterwards *ad infinitum* for targeted advertising which rapidly becomes a nuisance, or "spam".

In the same category is "adware", which brings advertisements to one's computer after one has clicked on a link in an Internet browser window. Even though many of these provide the facility to turn them off, some do not, which changes the "adware" to spam.

The ECT Act deals with spam in section 45, which imposes certain duties upon anyone who sends a consumer "unsolicited goods, services or communications". The sender has to provide the consumer with the option of cancelling his or her subscription to such mailing list (s 45(1)) and also with particulars as to how the sender obtained the consumer's personal information (s 45(2)). Section 45(3) criminalises the action of not complying with these two requirements

and s 45(4) criminalises the sending of unsolicited communications to a person after the latter has notified the sender that such communications are not welcome.

The above looks good in theory, and would probably work reasonably well on South African spammers, but most of the junk mail and spam come from overseas destinations and also from sources that do not respond to any attempted e-mail communications. Geissler *Bulk unsolicited electronic messages in South Africa* (LLD thesis Unisa 2005) recommends specific spam legislation based on an Australian model. She recommends that spam be defined as "unsolicited, bulk e-mail" and that the definition should not be limited to "unsolicited, bulk, commercial e-mail" (378). Other useful principles to be incorporated into such legislation include an "opt-in" rather than an "opt-out" approach (the ECT Act presently subscribes to the latter); proper consent; accurate sender information; a functional unsubscribe facility; immediate self-identification by messages as "unsolicited"; a prohibition of tools designed for transmitting spam and a prohibition on the practice of registering multiple e-mail addresses for purposes of unsolicited bulk e-mail.

5 Can the South African common law adapt to deal with these new examples of cyber crime?

How would our common law cope with the many new deceptive schemes dreamed up by cyber-criminals? In a series of articles on precisely this topic, Ebersöhn seems to be fairly optimistic on this score. In "A common law perspective on computer-related crimes" 2004 *THRHR* 22 ff the author argues that modern *theft* is flexible enough to encompass "the appropriation of personal rights" (31), the electronic transfer of credit between banking accounts (33), the copying of incorporeal property (37) and even passwords and confidential credit card information (42). While I applaud the creativity embodied in many of these arguments, and also feel that these are vital signs of life of a healthy criminal justice system, I feel that Ebersöhn should perhaps also have canvassed the question of *nullum crimen sine lege* (no crime without a prior law), also known as the legality principle. The adoption of South Africa's constitution has, in my opinion, considerably reined in the law-making ability of South Africa's courts.

In a follow-up article (2004 *THRHR* 193ff) Ebersöhn argues in a similar vein with regard to *fraud*. He makes out a strong argument that many computer-related schemes would fall within the wide parameters of "potential prejudice", but perhaps takes the matter a little too far when arguing that an unsuccessful hacking attempt constitutes the completed crime of fraud "because a risk of prejudice existed when the misrepresentation was made" (201 203). In my own opinion the already vague boundaries in the doctrine of inchoate crime between "the end of the preparatory actions" and "the commencement of the consumation" make poor bed-fellows with a concept as vague as "potential prejudice". Again the legality principle would seem to pose a few constitutional obstacles to extending the South African criminal law by analogy. Ebersöhn also argues that "South African courts have expanded the term 'property' to include 'substantial interests' as well as 'rights in such property', for the purposes of *malicious injury to property*" (207 – my emphasis).

In the final article in the series (2004 *THRHR* 375ff), Ebersöhn even argues that the crime of *crimen iniuria* might be committed by hacking into a computer system:

> "Therefore it is submitted that where a hacker gains access to A's computer system and copies, deleted, or modifies data he commits crimen iniuria. It is further submitted that where a hacker merely gains access to a computer system without deleting, copying or modifying data, he is also guilty of crimen iniuria" (379).

The author rounds off his article with an appeal to the constitutional right to privacy, but, as stated above, this right might have to be reconciled with another constitutional right, namely the right of any citizen to have the legality principle honoured by his or her lawgiver.

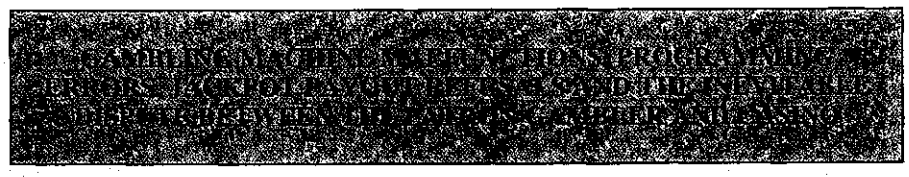
6 Conclusion

Hopefully this overview of the present cyber crime scene in South Africa has proved to be instructive. Despite the creative arguments of authors such as Ebersöhn, the most economic way forward (or "how to get the most feathers, with the least squawking") would probably be to amend South Africa's recent ICT legislation, in particular the ECT Act, so as to make them more useful.

Which amendments would be useful? Well, a raise in the criminal jurisdiction from twelve months to a few years would probably be useful. Ebersöhn's recommendation that the wording of section 86(5) be amended from committing "an act described in this section" to committing "an act with intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users" also seems useful. The anti-spam provisions of the ECT Act should also be amended urgently along the lines suggested above, seeing that spam is fast becoming one of the less desirable side-effects of electronic communication.

South Africa should also get its procedural obligations in terms of the Cybercrime Treaty in place, and should help to drive this important instrument against global cyber crime. A few common-sense initiatives such as these, particularly if one can get cooperation between the private sector and the government, would go a long way towards addressing cyber crime in South Africa and would help to protect the most valuable asset of all – data.

DANA VAN DER MERWE
University of South Africa



1 Introduction

The legal position with regard to malfunctioning machines, programming errors, jackpot payments, the subsequent dispute between the patron and the casino, as well as the procedure to be followed, are the subject of this note. Every once in a while a report appears in the press about a casino patron who believes that he has won a jackpot on the slot machines, only to be told by the casino that payment is