Chapter 38

Cyber law

'Things don't have to change the world to be important.'

Steve Jobs (1955–2011)
American businessperson

What is covered in this chapter

WHY THIS CHAPTER IS IMPORTANT

The impact of technology on business will change the way that commerce operates over the next century. Technologies such as video, telecommunications, and computers have already started to combine in ways that provide innovative alternatives to consumers for both their entertainment and commercial convenience.[1]

The world wide web was invented in 1991. Who would have thought in such a short time that your cellphone would also be a gateway to the internet? That your cellphone would allow you to buy groceries online, shop for clothes anywhere in the world, download movies and music, and that paying with cash money at a shop would be redundant because you could just swipe your phone over the electronic sensor and the amount would be deducted automatically from your bank account?

Nowadays, the world shops more online than it does face-to-face. The internet knows no physical boundaries and no territorial borders. This has lead to new concerns about the enforcement of various laws based on the principle of territoriality. How can one enforce a contract entered into over the internet? Which court has jurisdiction? Who pays VAT?

1 Hahn, H, *The Internet Complete Reference*, 2nd edition, Berkeley: Osborne McGraw-Hill 1996, 1–32.

Existing legal principles relating to trademarks, copyright, privacy, obscenity, and defamation are being strained to deal adequately with the challenges posed by the internet.

This chapter will discuss basic internet issues, as well as the way South African law is evolving to deal with the problems of regulating the way people enter into contracts and conduct themselves online.

CYBER LAW

1 Intellectual property issues

1.1 Domain name and trademarks

The domain name is a very important part of corporate identity on the internet. It is:

- The address for sending and receiving e-mail.
- The starting point for searching the internet.
- The symbol for recognition of products and services.

There are three parts to the domain name, each separated by a full stop. For example, in 'companyname.co.za', the three parts, in order, are:

- The company name.
- The top-level domain name. This indicates the type of corporate entity. For example, 'com' or 'co' means a commercial organisation, 'ac' means academic institution, 'gov' means government, 'org' means a non-profit organisation, and 'mil' means a military institution.
- The second-level domain name. This indicates the country of origin. For example, 'za' means South Africa, 'uk' means the United Kingdom, and 'au' means Australia. In the United States, the second level domain name is usually not used.

Domain names are allocated to applicants by regional authorities on a first-come, first-served basis. A requested name may be allocated provided it is not identical to one already registered.

Registration excludes anyone else from using that domain name. This means that it is possible for an applicant to register a domain name that is a well-known trademark owned by another, and by doing this may exclude the trademark owner from using the domain name on the internet.[2]

Where the domain owner has no legitimate reason for the registration of the name, existing legal remedies based on unfair competition and trademark violations allow the courts to deal with disputes. In terms of our law, and specifically the Trade Marks Act,[3] a 'mark' includes any sign capable of being represented graphically. This means that a domain name serves the same purpose as a trademark, and may be registered as a trademark. Accordingly, our law appears sufficient to deal with domain names that are confusingly similar to registered trademarks.

2 Kent, P, The Complete Idiot's Guide to the World Wide Web, Indianapolis, IN: Alpha Books 1995, 1–36; 'Cyberlaw – the Internet and the Law', *Business Blue-Book of South Africa*, Cape Town: National Publishing (Pty) Ltd 2002.

3 Trade Marks Act 194 of 1993.

To avoid litigation, domain names should be registered in respect of names that one wishes to use now, and also names that one may wish to use in future.

Even though it is possible for the purposes of the Trade Marks Act[4] to classify a domain name as a mark and deal with any infringements under the Act, trademarks and domain names are different. For example, the same or similar trademarks can validly be registered in respect of different goods and services, provided that the trademarks do not cause confusion or deception in the mind of the public. However, once a domain name is registered, that is the only name that can be registered in the particular domain-name space.

A domain name can create a lot of goodwill and can be very profitable. Profitability may be increased if the website uses a domain name with a respected or well-known trademark. A 'cybersquatter' is someone who registers a domain name using another's trademark or other intellectual property and then attempts to sell the domain name to the proprietor – a situation that can result in considerable cost to the trademark owner.[5]

A trademark owner may find itself unable to register a domain name incorporating its trademark because someone else already registered the domain name previously. The trademark owner is then faced with a situation where it has to pay the cybersquatter a large price for the use of its own domain name.

The South African body which allocates and registers domain names in the .co.za domain, Uniforum SA (Pty) Limited, does not have the capacity to investigate whether the domain name that is sought to be registered infringes another's intellectual property rights. An international body called the Internet Corporation for Assignment of Names and Numbers (ICANN) uses arbitration to resolve these cases. The arbitrator can order a domain name to be cancelled and transferred to the rightful owner.

Currently, four organisations may be used as arbitrators:

- CPR Institute for Dispute Resolution (CPR).
- Disputes.org/eResolution consortium (DeC).
- The National Arbitration Forum (NAF).
- The World Intellectual Property Organisation (WIPO).

In 2006 the Alternative Dispute Resolution (ADR) Regulations[6] were published in the *Government Gazette* to resolve disputes relating to .co.za domain names. This made it possible to lodge complaints in respect of .co.za domain names registered at any time either on the basis that it is an abusive registration or that it is an offensive registration. Model complaints and answers, with details of information that should be submitted are set out in the regulations.

Within 20 days of the commencement of the dispute, the registrant is required to submit a response and thereafter the complainant has five days within which to submit a reply. The ADR provider will then appoint one to three adjudicators. The adjudicator will send their decision to the ADR service provider within 14 days. It is possible to appeal the decision of a single adjudicator.[7]

A complainant must prove that:

- The domain name registrant has registered a domain name incorporating the

4 Trade Marks Act 194 of 1993.

5 Viljoen, M, In pursuit of the cyberpirates – The new ADR system for .co.za domain name complaints, *De Rebus*, Pretoria: Law Society of South Africa October 2007.

6 Government Notice R11666 in *Government Gazette* 29405/22-11-2006.

7 Viljoen, M, In pursuit of the cyberpirates – The new ADR system for .co.za domain name complaints, *De Rebus*, Pretoria: Law Society of South Africa October 2007.

complainant's trademark and that the domain name is identical or confusingly similar to a trademark in which the complainant has rights;
- The domain name registrant has no rights or legitimate interest in the domain name; and
- The domain name has been registered and used in bad faith.

African National Congress v Umwembi Communications[8]

In 1997, three employees of the ANC who administered the domain name anc.org.za as part of their duties formed a company to provide IT services to the ANC. After years of disputes about payment of R32 million for hosting and developing the party's website and membership system, a settlement agreement was entered into in 2018 providing that the domain records would remain with U until payment was received, and that within 24 hours of payment the domain property would be transferred to the ANC.

U argued that it had been the lawful owner of the domain name since it was established in 1997. In terms of the settlement agreement reached with the ANC, it had been specifically agreed that the domain name and records would remain the property of U until the final payment was received from the ANC.

The Tribunal held that the ANC had not provided any evidence of any rights to the domain name, nor that it gave any instructions to U to register or renew the domain name on its behalf. Further, that the ANC had presented no evidence that it had any rights to the name or mark of 'ANC'.

The dispute was therefore refused and the ANC failed to recover the domain name.

Examples of circumstances that will be considered to be evidence of the bad-faith registration and use of a domain name:
- Circumstances indicating that the domain name was registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of the domain name registrant's out-of-pocket costs directly related to the domain name.
- The domain name was registered in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the domain name registrant has engaged in a pattern of such conduct.
- The domain name was registered primarily for the purpose of disrupting the business of a competitor.
- By using the domain name, the domain name registrant intentionally attempted to attract for financial gain, internet users to the registrant's website or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of the registrant's website or location of a product or service on the registrant's website or location.

Nandos International Limited v M Fareed Farukhi[9]

A leading case involved the domain names nandos.com and nandoschicken.com, held by a California, United States resident, Fareed Farukhi. It was alleged by Nando's that Farukhi's conduct

8 *African National Congress v Umwembi Communications SAIIPL Decision* [ZA2018-0350] 31 January 2019.

9 *Nandos International Limited v M Fareed Farukhi* Case No D2000-0225 WIPO Administration and Mediation Center Administrative Panel Decision May 23, 2000.

amounted to a carefully planned and calculated step to take unfair advantage of the international repute and goodwill of the Nando's trademarks.

Evidence was led that the company Nando's Chicken had traded using these trademarks since 1989. Nando's claimed an international reputation emanating out of its use of these trademarks.

Nando's approached Farukhi in an attempt to acquire the subject domain names. It appeared that he had never used the registered domain names and he indicated to the complainant that he wanted to license the use of or sell the domain names to Nando's. Farukhi's defence was that his ethnic origins are in southern India, hence the alleged use of a word in the Kannada language. He alleged that the word 'nandos' means 'ours' or 'mine', and that he intended to set up a web portal for the subcontinent. After acquiring the nandos.com name from a prior registrant, Farukhi proceeded to register 'nandoschicken.com'.

The arbitration panel found that the most damaging evidence against Farukhi was the fact that after obtaining the right to the domain name, 'nandos.com', he had personally registered the domain name, 'nandoschicken.com'. If it was a coincidence that he obtained the domain name 'nandos.com' when he had never heard of Nando's, the trademark of the company with the international reputation for selling chicken, it was extraordinary that he should again, as a coincidence, register the domain name 'nandoschicken.com'. The registration of nandoschicken.com was strong evidence that the respondent had knowledge of the business operation of the holders of the Nando's and Nando's Chicken trademarks. Registration or holding of both domain names by the respondent, in the view of the panel, clearly showed that he intended either to sell the names to the complainant or to a third person who would do so, or that he wanted to engage in a business which would associate its products with those of the complainant's trademark.

The panel proceeded to find that the objective of the respondent, Farukhi, was in bad faith and ordered the domain names 'Nandos.com' and 'Nandoschicken.com' to be transferred to the complainant.

1.2 Metatags

'Metatags' are descriptive keywords that are inserted in the source code of websites to enable internet search engines to identify a particular site. They cannot be seen by an internet user. Their value lies in their ability to optimise internet searches. Depending on the number of corresponding metatags contained in a website's source code, a website may be ranked ahead of another in a list of search results. Advertisers use this hidden system to maximise their exposure on the internet.[10]

Courts in Europe and the United States have held that the covert use by a company of a competitor's trademark as a metatag amounts to trademark infringement.[11]

1.3 Copyright

General principles of South African copyright law apply. This means that no one may copy or distribute the content of their own website when it contains material by an author other than that of the website owner themself without first obtaining the necessary permission, unless the use is for study, private use, or criticism or review. Even then, the amount of material copied must be justifiable and both the identity of the author and the source must

10 Burt, H, Metatags, *De Rebus*, Pretoria: Law Society of South Africa December 2003.

11 *Reed Executive plc and another v Reed Business Information Limited and others* [2002] EWHC 2772; *Niton Corporation v Radiation Monitoring Device Inc* 27 F.Supp. 2d 1066 (D Mass 1998); *Playboy Enterprises Inc v Terri Welles et al* 78 F.Supp. 2d 1066 (SD Calif. 1999); 162 F.3d 1169 (9thCir).

be acknowledged. However, the law is virtually powerless to prevent material on websites from being copied and distributed worldwide.[12]

Software can be downloaded from the internet which allows for software swapping. Since 2006, the most popular way for people to share software, movie and music files has been through bittorrent sharing. Bittorrents or 'torrents' work by downloading small pieces of files from many different internet addresses at the same time. Each piece has instructions, read by your computer, on how to assemble the complete file once all the pieces have been downloaded. Because it is so easy to use, free from advertisements and costs nothing, it has been very unpopular with authorities and copyright holders. Bittorrent networking is by far the most popular use of the internet today.

Torrent software can be found using Google and downloaded for free. Once installed, the software allows users to look for any particular file they want, and will search the internet to find other computers from which to download the torrents. In return, your computer may be contacted by other computers and be requested to upload torrents. Downloading from others, and uploading to others, is what is meant by 'peer-to-peer' or 'P2P' sharing.

Whereas searching for torrents and P2P sharing technology is legal, many files available online are protected by copyright. Intellectual property laws in nearly all countries prohibit downloading torrent files of copyright material.

Companies that knowingly allow employees to use their broadband facilities to download music, movies or software could potentially also face litigation.

The internet is challenging traditional concepts of copyright. As broadband technology becomes available in South Africa, the constraints imposed by the size of files will diminish.

1.4 Hyperlinks

It is possible for an internet website (primary site) to contain highlighted text indicating the name of another website (secondary site), or even include a small picture (icon) of another website. By clicking on the highlighted text, or icon, it is possible to go directly from the primary site to the secondary site, without first having to type the secondary site page's address or Uniform Resource Locator (URL) of the web page the viewer wishes to access. This link is known as a 'hypertext' link.

Problems may occur when a secondary site owner objects to a primary site owner including a hypertext link:

- The secondary site owner may regard the content of the primary site as offensive.
- The hypertext link may bypass advertising material included on the secondary site, through a process known as 'deep-linking'. Advertising material is most often found on the first page (home page) of a website. By linking to a page further within the website, the ability of the primary site owner to obtain advertising revenue may be compromised.
- The logical flow of material is interrupted. This may affect the image of the product, service, or organisation.

Ticketmaster Corp v Tickets.com Inc[13]

In this US case, the plaintiff brought an action to prevent Tickets.com Inc from using hyperlinks to Ticketmaster's web pages. The plaintiff had exclusive arrangements for events marketed on its

12 Ebersöhn, G, The Unfair Business Practices of Spamming and Spoofing, *De Rebus*, Pretoria: Law Society of South Africa July 2003; 'Cyberlaw – the Internet and the Law,' *Business Blue-Book of South Africa*, Cape Town, National Publishing (Pty) Ltd 2002.

13 *Ticketmaster Corp v Tickets.com Inc* 2003 CorpLDec 28,607.

website, tickets for which were not available other than through it. By using deep-linking, the defendant had directed users to the Ticketmaster site where the tickets could be bought. The home page of Ticketmaster was bypassed. The Ticketmaster website had terms and conditions that prohibited deep-linking by unauthorised third parties.

The single judge of the Federal District Court of California stated that the deep-linking did not constitute copyright infringement as Tickets did not actually copy any portion of the Ticketmaster site but transferred users directly to the relevant Ticketmaster web page. Further, the court held that the act of deep-linking did not itself constitute unfair competition as Tickets did not mislead users as to the source of where the tickets could be purchased.

The court also held that because the terms and conditions were placed at the bottom of the Ticketmaster website and that since users were not required to consent to such terms and conditions, such as by clicking on an 'I accept' button, such terms and conditions did not create a legally binding contract between Ticketmaster and the user.

Some academics support hyperlinking because it increases traffic to a site. This is consistent with the philosophy of the internet being an open and free environment for the sharing of information, and access to information.

Critics say that deep-linking diverts visitors from a site's front or home page, resulting in fewer users seeing the advertising, disclaimers and navigation appearing on the home page. Further, it allows a third party unlawfully to benefit from the effort and time put into a website by the proprietor of the website.[14]

***eBay Inc v Bidders Edge Inc*[15]**

In this US case, the court dealt with the issue of internet privacy and trespass. The defendant collected information about online auctions and directed users to the best deal. eBay wanted to interdict the defendant from accessing eBay's website to collect data about items for sale. eBay argued that the defendant's conduct infringed their right of privacy and that eBay had the fundamental right to stop unauthorised and harmful access to its site.

The court ruled that the use of automated search programs known as 'bots' to collect information from websites amounted to trespassing.

The legality of hyperlinking and deep-linking have not been tested by South African courts. There is currently no legislation in South Africa preventing, prohibiting or regulating linking and deep-linking. Generally, our legislation regulates a physical environment, and not a virtual environment. For example, the Trespass Act[16] regulates the entry or presence on land or in buildings, and has not yet been interpreted to apply online.

1.5 Banner advertising

This takes place where the internet service provider (ISP) hosting a website displays a large advertisement for goods, products or services at the top or on the side of the computer screen image of the web page.

Disputes may arise where the banner advertises a competing, distasteful or unlawful product or service.

14 Ebersöhn, G, The Unfair Business Practices of Spamming and Spoofing, *De Rebus*, Pretoria: Law Society of South Africa July 2003.

15 *eBay Inc v Bidders Edge Inc* 100 F.Supp.2d 1058 (2000).

16 Trespass Act 6 of 1959.

There is currently no South African case law or legislation regulating this conduct by an ISP. In the absence of legislation, it has been argued that the right to advertise on a web page should be regulated by the terms and conditions of the contract with the ISP, and if advertising is to be allowed, the contract should specify the permitted manner of advertising.[17]

1.6 Framing

This technology allows multiple windows (frames) to be used independently of each other on a computer screen. Numerous frames are used to access different websites. By combining with hyperlinks, advertising on the primary site can remain in display as a border or frame to the secondary site.

Problems may occur when a secondary site owner objects to a primary site owner using framing, particularly when the secondary site owner's advertising is not displayed properly.

If used at all, hypertext links and framing should be used only with the permission of the secondary site owner, and should direct users to the home page of another website. Framing and linking also should be restricted by providing prominently displayed contractual terms and conditions of use on the website page.

2 What constitutes agreement on the internet?

Contracts entered into over the internet have the same legal validity as any other contract. In terms of the Electronic Communications and Transactions Act[18] it is possible for parties to enter into a valid contract by an 'electronic transaction'. This is an agreement where information is generated, sent, received or stored by electronic means, and includes a voice where the voice is used in an automated transaction, a web page or a stored record.

2.1 Agreements that must be in writing

The Electronic Communications and Transactions Act also makes provision for the governance of most electronic transactions. Contracts that by law must be in writing and which must be signed can be entered into electronically with certainty about enforceability.

The Act states that the requirement of 'being reduced to writing', which is required for some contracts, will be satisfied if the document or information is in the form of a data message, and is accessible in a way so that it can be reviewed again.

For example, a contract for the alienation of land can be concluded electronically if a data message is transmitted between the seller and the purchaser, capable of being stored by either or both parties, and capable of being retrieved indefinitely for subsequent use.[19]

2.2 Digital signature

The traditional approach of our courts regarding signatures on written documents has been pragmatic, and based on authenticating the identity of the signatory. In the days before electronic communications, courts have accepted any mark made by a person attesting to a document as a valid signature.

17 Ebersöhn, G, The Unfair Business Practices of Spamming and Spoofing, *De Rebus*, Pretoria: Law Society of South Africa July 2003.

18 Electronic Communications and Transactions Act 25 of 2002.

19 Rens, A, Approach with Caution, *De Rebus*, Pretoria: Law Society of South Africa June 2003.

The Electronic Communications and Transactions Act aims to give the same legal effect to digital signatures that traditional signatures enjoy in our law. The Act identifies two different types of signature that can be used in electronic communication:

- **Electronic signature**: This is data associated with the electronic message and is logically intended by the user to be a signature – for example, a typed name at the foot of an e-mail. This is because it identifies the person, is logically associated with the message contained in the e-mail, and therefore is an electronic signature. Another example of an electronic signature is the scanned image of your handwritten signature embedded into a document.[20]
- **Advanced electronic signature**: This involves a form of accreditation of an electronic signature by a specialist accreditation authority. Only once the electronic signature has been accredited will it be certified as an 'advanced electronic signature'. Accreditation is a process that involves an application and submitting documents to the accreditation authority. Sometimes extra security can be added to ensure that the advance electronic signature is authentic. For example, a special private key can be used to generate the signature, and special software can be used to ensure that the communication and signature have not been tampered with.

***Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another*[21]**

The parties entered into a written contract that contained a non-variation clause providing that no variation or consensual cancellation would be effective unless reduced to writing and signed by both parties. After this, over the course of several e-mails, a dispute arose as to whether or not the agreement had been cancelled by e-mail.

One of the parties argued that the e-mail exchange was simply a negotiation between the parties and did not amount to cancellation of the contract; further, that because the Act required an advanced electronic signature and none of the e-mails had such advanced signatures, the agreement could not have been cancelled by e-mail.

The court held that the e-mails were reliable, conveyed information accurately, and clearly showed an intention to cancel the agreement. Further, the typed written names of the parties at the foot of the e-mails were intended to identify the parties and were logically connected to the content of the e-mails. Accordingly, they constituted a valid electronic signature. As the parties had not specified the type of electronic signature to be used, no advanced electronic signature was required. The contract was validly cancelled.

The Act makes a distinction between two situations involving signatures in electronic contracts:

- Where the law requires a signature. Where the law does not specify the type of signature to be used, an 'advanced electronic signature' is required.
- Where the parties themselves agree on the added formality of a signature. Where the parties do not specify the type of electronic signature to be used, an 'advanced electronic signature' is not required. All that is necessary is that the person was identified and the person approved of the communication, and that in the circumstances the method used was appropriately reliable.

20 Manyathi-Jele, N, SCA rules that e-mail contract cancellation legal, *De Rebus*, Pretoria: Law Society of South Africa January/February 2015.

21 *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another* 2015 (2) SA 118 (SCA).

Global & Local Investments Advisors (Pty) Ltd v Fouché[22]

Nick F gave a written mandate to G to act as his agent, and invest money on his behalf. The written mandate stipulated that 'All instructions must be sent by fax to [a designated number] or by e-mail to [a designated e-mail address] with client's signature.' G received three e-mails with instructions to transfer money: two ended with the words: 'Regards, Nick' while the third ended with 'Thanks, Nick'. Acting on the instructions, G paid out a total of R804 000.

G argued that had complied with the mandate that came from the legitimate e-mail address of Nick F, and that the typewritten name 'Nick' at the bottom of the e-mails satisfied the signature requirement of the Electronic Communications and Transactions Act.[23]

The court held that the mandate had specifically required the signature of Nick F for a valid instruction, and not merely an e-mail or fax message purporting to be sent. The parties had not agreed to accept an electronic signature as envisaged by the Act; the parties had required a signature. The court held in favour of Nick F.

The Act provides that where an advanced electronic signature has been used, it will be regarded as valid and to have been applied properly, unless the contrary is proved. Agreement can also be constituted by an automated transaction where an electronic agent is used for one or both parties. If one of the parties to an automated transaction is a natural person, the natural person must be given an opportunity to correct a material error or else the contract will not be valid.[24]

Provision is also made for the use of advanced electronic signatures by notaries and commissioners of oaths to perform their duties online. A commissioner of oaths can now, in terms of the Act, provide someone with an electronic copy of a document that 'exists in paper or other physical form', and certify that the electronic copy of the document is a true copy of such a document, by using an advanced electronic signature.

2.3 Incorporation by reference

The common-law rule of 'incorporation by reference' is also included in the Act. However, the following criteria must be met before a data message, incorporated by reference, will obtain legal recognition under the Act:

- The data must be incorporated into a data message.
- The data must be referred to in such a way that a reasonable person would have noticed its reference and incorporation.
- The data must be made accessible to the other party in a form in which it may be read, stored and retrieved by the other party.

2.4 Delivery

The Electronic Communications and Transactions Act also makes provision, by involving the Post Office as a third party, for information or a document to be sent by registered or certified 'mail' to the address supplied by the sender.

2.5 Offer and acceptance

An 'offer' is deemed to have been made when one of the following happens:

- The data message containing the offer is received.

22 *Global & Local Investments Advisors (Pty) Ltd v Fouché* 2021 (1) SA 371 (SCA) (Mojapelo AJA (Navsa, Saldulker, Makgoka and Nicholls JJA concurring)).

23 Electronic Communications and Transactions Act 25 of 2002.

24 Ibid.

- The data message is entered into an information system outside the control of the originator.
- The data message can be retrieved by the addressee.

The Electronic Communications and Transactions Act presumes a data message to have been 'received' by the addressee when the complete data message enters an information system used for that purpose by the addressee and can be retrieved and processed by the addressee.[25]

The Act[26] adopts the Reception Theory of contract – a contract is concluded at the place where and at the time when a data message which contains the acceptance of an offer is received by the offeror. The parties can agree to a different manner of acceptance.

The most widely used forms of agreement used on the internet are 'click-wrap' and 'browse-wrap' agreements. In a click-wrap agreement one person clicks on words or an icon stating 'I agree'. The terms and conditions of the contract may be available by browsing online through a link or may be visible on the same internet page. In a browse-wrap agreement, the site merely states that any agreement is subject to various terms and conditions, but does not ask the person specifically if they agree. In other words, the terms and conditions are incorporated by reference.[27]

2.6 Identity of the offeror

Concerning the origin of the message, the Electronic Communications and Transactions Act further provides that a data message will be deemed to be that of the originator if it was sent:

- By the originator personally.
- By a person who had authority to act on behalf of the originator.
- By an information system programmed by or on behalf of the originator to operate automatically and that information system operated in accordance with the programming.

2.7 Reality of consent

The Electronic Communications and Transactions Act further provides for certain contracts to be void in the instance of mistake. This operates where:

- A natural person made a material error in the data message and the electronic agent (representing the other party) did not provide an opportunity to prevent or correct the error.
- That person notifies the other person of the error as soon as practicable after learning of it.
- That person takes reasonable steps to return the performance tendered, including steps in accordance with the other person's instructions to return the performance received.
- That person has not used or received any material benefit or accepted performance, if any, from the other person.

25 Rens, A, Approach with Caution, *De Rebus*, Pretoria: Law Society of South Africa June 2003.
26 Electronic Communications and Transactions Act 25 of 2002.
27 Collier-Reed, D and Lehmann, K, *Basic Principles of Business Law*, 2nd edition Durban: LexisNexis, September 2010.

3 Consumer protection for contracts over the internet

The Electronic Communications and Transactions Act[28] creates legal certainty about the validity of electronic transactions and contracts.[29]

The Act protects consumers in South Africa who contract online with merchants irrespective of where the merchant is located. The Act also requires all retail websites to detail their security procedures and privacy policies in respect of payment and personal information.

Online retailers are required to use a payment system that is sufficiently secure. A supplier who does not use a secure payment system could be held liable for any damages sustained by a consumer in this regard.[30]

The Act protects consumers who are natural persons by requiring vendors using websites for electronic transactions to provide 18 pieces of information, including the following:[31]

- The supplier's full name, legal status, physical address and telephone number, website address and e-mail address, registration number and place of registration, and address for service of legal documents.
- Details of the supplier's membership of any association that provides for rules for self-regulation of members, with contact details; code of conduct to which the supplier belongs and how the code may be viewed online.
- The complete terms of the agreement applicable to the transaction.
- Any guarantees given and how the terms may be viewed online.
- A description of the goods or services for sale.
- The full purchase price of the goods or services including all taxes and fees.
- Manner of payment.
- Time for delivery.
- The return, exchange and refund policy of the supplier.
- Details of how the consumer can get a full copy of the transaction record.
- Details of the alternate dispute resolution policy and how the terms can be viewed online.
- Details of security and privacy policies and procedures regarding payment and personal information.
- Minimum duration of contracts to provide goods or services on an ongoing basis.
- Details of any relevant cooling-off period.

Consumers must be given the opportunity to review any proposed transaction, to correct any mistakes, and to withdraw before finalising the order.

In addition, all consumers must be given a cooling-off period of seven days to cancel an online transaction without reason or penalty, and to get a refund, subject to the deduction of specific costs. The cooling-off period does not apply to contracts for financial services; auctions; food or beverages; goods made to the customer's specifications; books, newspapers or magazines; software, audio or video products that have been unsealed; gambling or lottery

28 Electronic Communications and Transactions Act 25 of 2002; Stassen, P and K, *De Rebus*, New Legislation, Pretoria: Law Society of South Africa November 2002.

29 Rens, A, Approach with Caution, *De Rebus*, Pretoria: Law Society of South Africa June 2003.

30 E-Commerce, *Business and Investment in South Africa*, Sandton: Cliffe Dekker Attorneys, May 2005.

31 Collier-Reed, D and Lehmann, K, *Basic Principles of Business Law*, 2nd edition Durban: LexisNexis, September 2010; E-Commerce, *Business and Investment in South Africa*, Sandton: Cliffe Dekker Attorneys, May 2005.

services; or accommodation, transport, catering or leisure services for a specified date or time period.

Failure to provide any of the required information will result in an automatic right by the consumer to cancel and withdraw from the contract within 14 days after receiving the goods or services. A supplier must process the order within 30 days of receipt, failing which the consumer may cancel by seven days' written notice.

The Electronic Communications and Transactions Act[32] is also covered in chapter 29: '*Consumer protection*'.

4 Unsolicited e-mail and SMS communications

4.1 What is spam?

'Spam' is the name given to unsolicited commercial communications. The term is used to describe e-mail or SMSs. In the context of e-mail, spam usually means unsolicited commercial e-mail or unsolicited bulk e-mail.

'Unsolicited' means that the receiver has not granted verifiable permission for the message to be sent. 'Bulk' means that the message was sent as part of a larger collection of messages, all of which have substantively the same content. Because it costs very little to send spam, each spam communication costs the consumer more to receive in terms of money and resources than it costs the sender to send.

Spam is a problem because of the amount of spam that is sent – it amounts to approximately half of all e-mail traffic. Apart from the productivity costs for business and the internet community, the traffic of spam also blocks computer systems and networks.

Any electronic message will be considered spam if all three of the following factors are present:

- The recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients.
- The recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent.
- The transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

Section 45 of the Electronic Communications and Transactions Act[33] requires the sender of an unsolicited commercial communication to comply with the following three requirements:

- To provide the consumer with the option to cancel their subscription to the mailing list.
- To furnish the consumer at their request with the identifying particulars of the source from which the consumer's personal information was obtained.
- Not to send a second unsolicited commercial communication to a person who has advised the sender that the communications are unwelcome.

32 Electronic Communications and Transactions Act 25 of 2002.
33 Ibid.

4.2 Potential liability for spam

If a sender does not comply with section 45 of the Electronic Communications and Transactions Act[34] they are guilty of an offence and liable on conviction to a fine, or a maximum of 12 months' imprisonment.

One potential problem is that of jurisdiction. Because most spammers operate from the US, Europe and the Far East, it could be argued that South African law does not apply to spammers in these countries. Despite this, in some cases certain spam-related activities could also be covered under the Act, or other laws. For example:

- Forgery of message headers, which is also called 'spoofing', could be a crime under section 86(2) of the Act, which makes the intentional and unauthorised interference with data in a way that causes such data to be modified a criminal offence.
- Sometimes so much spam can be sent that it constitutes an assault on a network. This will be the case where the spam floods the network with so many additional requests, that regular traffic is either slowed or completely interrupted. Spam that causes an e-mail server to crash could be considered a denial of service that also constitutes a cyber crime under section 86(2) of the Act, as it constitutes an unauthorised interception or interference with data.
- Senders who use trademarked material in their unsolicited communications without permission could be violating trademark laws or they may find themselves to be guilty of passing off in terms of common law.

The effectiveness of the Act in preventing spam has been criticised:[35]

- The Act only offers protection to consumers who are spammed. However, the Act defines a consumer as a natural person. This creates problems if spam is sent to legal persons such as companies or close corporations.
- It is unclear whether or not the sender must provide the option to cancel (whether in the form of an e-mail address or a hyperlink to a website) in the first e-mail sent. The issue is important because the sender can be guilty of a criminal offence where they act innocently. For example, where the sender simply forgets to provide the option to cancel in their first electronic communication. The effectiveness of an opt-out request can be debated, as all it often does is confirm the existence of the e-mail address being spammed.
- The Act does not require that the sender provide accurate details of their name or physical or electronic addresses.
- There is no definition as to what is 'unsolicited'. In general a communication is considered to be unsolicited if there is no prior relationship between the parties; the consumer has not expressly consented to receive that communication; and the consumer has previously tried to terminate the relationship, usually by instructing the sender not to send any more communications in the future.
- There is no definition as to what constitutes 'commercial'. This is generally defined in terms of message content, rather than the intention of the sender in sending the communication. Examples of unsolicited communication of a commercial nature that should not be subject to criminal sanction include those that do not include or promote illegal or offensive content; do not have a fraudulent or otherwise deceptive purpose; do not collect personal information; are not sent in a manner that disguises

34 Electronic Communications and Transactions Act 25 of 2002.

35 Rens, A, Approach with Caution, *De Rebus*, Pretoria: Law Society of South Africa June 2003.

the originator; and offer a valid and functional address to which consumers can send messages opting out of receiving further unsolicited communications. There are many varieties of non-commercial spam including charitable fundraising solicitations, opinion surveys, religious messages, political advertisements, virus hoaxes and other urban legends and chain letters.
- Since the real problem with spam is in the volume of e-mail messages, and not their content, measures need to be put in place to deal with unsolicited bulk e-mail as well. The main issue is how many copies of a message are sent and within what time period they are dispatched, for them to qualify as a bulk transmission.

Aspects of the Electronic Communications and Transactions Act[36] are also covered in chapter 29: '*Consumer protection*'.

5 Protection of personal information

The Electronic Communications and Transactions Act[37] provides for privacy issues in the form of a code or a set of principles to which data controllers may voluntarily subscribe. Any data controller who intends to subscribe to the voluntary code must subscribe to all the principles, and not just to parts of the code.

The provisions of the code record that a data controller must:
- Obtain permission to record personal information.
- Disclose the purpose for which he seeks the information.
- Not collect information that is irrelevant to the data subject.
- Refrain from using the information for any other purpose.
- Keep a record of at least one year after collection of what the information was and the purpose for which it was collected.
- Not disclose the information without permission.
- Destroy all such information when it becomes obsolete.

The provisions of the Protection of Personal Information Act 4 of 2013 are discussed in chapter 39: '*Privacy*'.

6 Legal consequence of unlawful invasion of privacy

Computers do not have limitations associated with storage and the data is easily accessible. This allows for subtle, pervasive and intrusive forms of privacy invasion, in the collection, access, use and dissemination of personal information.

These may arise in a variety of forms:

6.1 Criminal sanction

A contravention of the Regulation of Interception of Communications and Provision of Communication-related Information Act[38] provides generally for a fine, or to imprisonment for a period not exceeding two years. Section 2 of that Act states that no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to

36 Electronic Communications and Transactions Act 25 of 2002.
37 Ibid.
38 Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.

6.2 Delictual liability

An employer can be held liable in delict if an employee intentionally or negligently forwards a virus by e-mail to another company. The employer may be liable should the recipient be able to show that the sender caused damage, that such damage arose negligently and that the individual concerned acted within the course and scope of their employment.

Harvey v Niland and others[39]

H and N were the only members of a close corporation. The CC employed them both, along with others, to provide specialist hunting services to trophy hunters. After the two argued, N left the employment of the CC (but remained a member) and was employed by a rival hunting company. H suspected that N was trying to steal clients. Another employee advised H that she knew of N's password for Facebook. She used the password, and provided H with copies of N's Facebook posts indicating that N was sourcing business for his new employer.

H applied to court to interdict N from breaching his fiduciary duties to the CC.

N argued in defence that s14(*d*) of the Constitution[40] provides for a fundamental right to privacy which includes the right not to have the privacy of communications infringed. N said he never gave his password to anyone, and that H had accessed his Facebook communications unlawfully in violation of section 86(1) of the Electronic Communications and Transactions Act,[41] which provides that 'a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence'. As the Facebook evidence had been unlawfully obtained, N argued it should be inadmissible.

The court examined the common-law rules of admissibility of evidence; in particular the rule that stated all relevant evidence which was not rendered inadmissible by an exclusionary rule was admissible in a civil court, irrespective of how it was obtained.

The court held that this rule was not absolute, but subject to a discretion to exclude unlawfully obtained evidence. In exercising that discretion, all relevant factors must be considered. These included the extent to which, and the manner in which, one party's right to privacy (or other right) has been infringed; the nature and content of the evidence concerned; whether the party seeking to rely on the unlawfully obtained evidence attempted to obtain it by lawful means; and the idea that 'while the pursuit of truth and the exposure of all that tends to veil it is cardinal in working true justice, the courts cannot countenance and the Constitution does not permit unrestrained reliance on the philosophy that the end justifies the means.'[42]

The court held that without the Facebook material, H had no case, and that it would have been entirely impractical for him to proceed in another way that used lawful means. It held that N was only invoking his right to privacy because he had something to hide. The Facebook evidence was held to be admissible, and the court granted the order in favour of H.

7 Defamation

E-mail can easily contain defamatory statements and give rise to a claim for damages. Vicarious liability for defamation could under certain circumstances attach to the employer.

39 *Harvey v Niland and others* 2016 (2) SA 436 (ECG).

40 Constitution of the Republic of South Africa, 1996.

41 Electronic Communications and Transactions Act 25 of 2002.

42 Manyathi-Jele, N, 'Unlawfully' Obtained Facebook Communication Admissible in Court, *De Rebus*, Pretoria: Law Society of South Africa, April 2016 p 38.

Western Provident Association v Norwich Union Healthcare and Norwich Union Life Insurance[43]
In this English case, Norwich Union was sued for defamation after one of its employees sent an internal e-mail message that wrongly suggested that a competitor was close to insolvency. Although the e-mail message was initially transmitted on Norwich Union's own internal e-mail system, it was nevertheless inadvertently transmitted to third parties and found its way back to the Provident Society. By the time summons had been issued the e-mail messages had been deleted within Norwich Union. Western Provident obtained a court order forcing Norwich Union to search their back-up systems to retrieve the data.

The matter was settled before a final judgment was delivered, after Norwich Union accepted that it was responsible for what had been written on its system by employees and made an apology through the High Court. The company paid £450 000 as damages and costs to the Provident Society.

As a general principle, defamation over the internet is regarded as having been committed where and when the defamatory material is accessed. The 'single publication rule' also will apply, meaning that there will be only one cause of action, irrespective of how many times the defamatory material actually has been accessed.[44]

Based on litigation internationally, it would seem that a service provider will not be liable for defamatory material published by newsgroups or placed on electronic bulletin boards, provided that they do not edit any of the material. Generally, the distributor of defamatory material is not liable, since it does not act as the publisher of the material.

The factors to determine whether or not a distributor or service provider will be liable for defamation are the following:

- The extent to which it exercises control over the decision to publish the defamatory material.
- The nature and circumstances of the publication.
- Its previous conduct.

To help avoid liability, a service provider or distributor could consider exercising as little control as possible over the material. The use of software to screen the content of published material perhaps also should be avoided, as this can be seen as a form of active editorial control.

This decision is fraught with difficulty. The failure to exercise any control over content could potentially render the service provider or distributor liable for the publication or distribution of defamatory material on the basis of negligence, in that it had the ability to screen out the material, and failed to do so.

Employers also face difficulty in that they may be held vicariously liable for defamatory material published on their computer systems by their employees. Potential liability may be limited by ensuring that the website contains prominently displayed disclaimers of liability on the website page.

The law of defamation is dealt with in chapter 36: '*Delict*'.

43 *Western Provident Association v Norwich Union Healthcare and Norwich Union Life Insurance* 1997 (unreported).
44 Ebersöhn, G. Online defamation, *De Rebus*, Pretoria: Law Society of South Africa November 2003.

8 Bullying and harassment

The purpose of the Protection from Harassment Act[45] is to prevent harassment or abuse. Anyone who believes they are being harassed, or someone who has a material interest in the well-being of such a person, may apply for a protection order. Importantly, even a minor under the age of 18 may apply for such an order without obtaining consent from a parent or guardian.

'Harassment' has a wide meaning, and includes: physical or verbal abuse; watching and following the complainant at or near where they live, study or work; engaging in any form of verbal, electronic or other communication aimed at the complainant; sending or leaving written communication or objects any place likely to be brought to the attention of the complainant.

The remedy is also available to anyone who is subject to harassment electronically, by internet, social media sites, text messages or e-mail. The application process is simple: all that is needed is to complete a form at a magistrates' court, which automatically creates an interim protection order and a warrant of arrest; once issued, if the police find that the harassment continues then the harasser will be deemed to be guilty of an offence and must be arrested.

After two weeks, court officials call on the respondent to come to court to explain to a magistrate why a final protection order should not be granted. The magistrates' court may issue a directive and order an electronic communications service provider to provide it with the full name, identity number and address of the harasser sending the text messages, tweets or e-mails. Further, it may order a member of the SAPS to carry out an investigation into the harassment, with the aim of obtaining the name and address of a harasser whose personal details are unknown to the complainant.

Conviction by the court may carry a fine or imprisonment for up to five years.

9 E-mail

Employers have legitimate concerns that employees may use the employer's e-mail systems to defame others, engage in misconduct such as harassment, breach copyright laws, make statements about products or services amounting to warranties, or disclose confidential material to others.[46]

If an employer wishes to monitor internet and e-mail communications sent by its employees, a carefully worded internet and e-mail policy must be implemented and the consent of employees obtained.

The policy should include:

- A statement about whether the employer's e-mail and internet facilities are reserved exclusively for business use, or whether they may be used for limited, private purposes.
- A statement about whether the employer has the right to monitor and intercept employee electronic communications and to monitor employee internet usage.
- Method of monitoring and who will be authorised to monitor.

45 Protection from Harassment Act 17 of 2011.

46 Ebersöhn, G. Online defamation, *De Rebus*, Pretoria: Law Society of South Africa November 2003.

- The prohibition of using employer e-mail and internet facilities for the communication of offensive material. The nature of what is considered offensive should also be detailed, and may include hate mail, and defamatory, sexist, and derogatory material.
- The prohibition of downloading certain material from the internet.
- Measures to scan material downloaded from the internet for viruses.
- The prohibition of transmission of confidential or sensitive material over the internet.
- The prohibition of subscription to mailing lists other than for legitimate business purposes.
- A statement about whether back-up copies of the computer system will be accessed for monitoring purposes.
- Time periods for deletion of e-mail.
- Consequences for violation of the policy.

Employees must be advised of the potential liability an employee may face through using electronic communications. Internet and e-mail policies should be communicated to employees on noticeboards and through the e-mail system itself.

Contracts of employment also must be amended to include the details of the electronic communications policies, together with a specific consent to monitoring authorisation to be signed by the employee.

In the absence of an employee's express consent to monitoring, it is highly unlikely that an employer legally may monitor e-mail or internet communications. Further, unauthorised monitoring will be illegal and will probably be inadmissible in any disciplinary inquiry, civil action, or criminal prosecution.

10 Internet service providers

Internet service providers (ISPs) that manage consumers' e-mail through their servers, as well as organisations that run their own e-mail servers, can be liable for negligence if they fail to adhere to the standard of care legally required of them. In terms of our law the ISP would be negligent if a reasonable person in the position of an ISP:

- Could foresee the reasonable possibility of its conduct injuring a subscriber and causing them loss.
- Could take reasonable steps to guard against such occurrence.
- Fails to take such steps.[47]

The negligent conduct would be in the form of an omission, for example, by not taking technical steps to deal with the problem. Such steps could include not implementing subject line blocking, the use of blacklists and reverse domain name look-ups (establishing whether a sender is real).

The type of loss envisaged would include a situation where a virus attached to a spam e-mail, which passes through the ISP's e-mail server, deletes all the data on the subscriber's hard drive.

The taking of reasonable steps to guard against such an occurrence would include empowering their subscribers by assisting them to manage the spam problem by, for example, making spam filtering software and blacklists available, or by making facilities

47 *Kruger v Coetzee* 1966 (2) SA 428 (A) at 430 as cited in Neethling, Potgieter and Visser, *The Law of Delict*, 4th edition, Durban: Butterworths p 129.

available to report spam, as well as by making the subscribers aware of the issues, and in joint collaborative efforts with other interested bodies such as the South African Marketing Federation.

11 Labour law internet issues

The abuse of e-mail and internet facilities at work has a number of obvious risks which include:

- **Gender and racial issues**: The sending of material which has gender or racially sensitive content has serious implications for both the company and the employee who sent the e-mail. The CCMA has upheld the dismissal of employees who have distributed racist cartoons in the workplace.[48]
- **Sexually explicit material**: The viewing of sexually explicit material in the workplace has a direct impact on fellow employees who are often offended by this material. These types of complaints are usually dealt with via grievance procedures and often result in disciplinary measures being taken as a consequence of the employer's duty to protect employees from such conduct. Generally disciplinary action will take the form of sexual-harassment charges being made against the offending employee. The CCMA has frequently upheld the dismissal of employees who have visited pornographic websites using workplace computers.[49]

***Bamford and others vs Energiser SA Ltd*[50]**

A number of employees were dismissed after being found guilty at a disciplinary inquiry on charges relating to repeated receipt forwarding to other staff of obscene pornographic material and jokes. A manager had discovered on the company's computer system thousands of e-mails of a pornographic, racist and sexist nature, some of which carried the brand names of other companies. These e-mails had been stored by the dismissed employees on the company's computer system. The company contended that the use of its computers for this purpose had affected the efficiency of its computer system and that the storing of such material in its international network potentially compromised its brand name.

The arbitrator held that the employees should have been aware of the fact they should not be trafficking in offensive material, even if the company had no rules on this aspect at all. He also held that the parodying of trade names constituted a trademark violation that exposed the company to business risk, and rejected the employees' claim that the company had invaded their privacy because the messages were personal and private. He held that individuals had no right to deposit private material in an employer's storage facility and then prevent the employer from examining it to determine whether there is a point to it being preserved.

Abusive or racist social media postings made privately can also result in disciplinary sanctions at work.

48 *Cronje v Toyota Manufacturing* (2001) 21 ILJ 735 (CCMA).

49 *UASA v Khutala Coliery* Case Number NP14171; *Anandhroy Ramdin v Mondi Limited t/a Mondi Paper* Case Number KN44695 decision of the CCMA dated 14 October 2000.

50 *Bamford and others v Energiser SA Ltd* (2001) 12 BALR 1251 (P).

***Edcon Ltd v Cantamessa and others*[51]**

While on annual leave, C watched a TV programme regarding a cabinet reshuffle and posted a message on her personal Facebook page which referred to the government as monkeys. She was summarily dismissed.

C argued that she had used her personal computer while on annual leave, and that the employer's social media policy only applied to employees accessing the internet through company resources and during working hours. Also, even though she mentioned her employer on her Facebook profile, no reasonable person would associate her comment with her employer. She also argued that E had suffered no loss because of the post as she had only referred to the government, and E had been inconsistent by dismissing her while only giving final warnings to employees who 'liked' the post.

The Labour Court held that an employer may still discipline employees for conduct outside of the workplace if there is a connection between the employee's conduct and the employer's business. This connection was made because she identified herself as an Edcon employee. The court also held that the comment had exposed Edcon to reputational harm. The right to free speech did not extend to statements calculated to cause offence and harm and her frustration at government did not give her the right to express racist sentiments.

12 Cyber crime

Online criminal activity has increased significantly in the past decade, with 37% of South African companies reporting cyber crime in 2020. Law firms and legal practices have been targeted by cyber criminals, with insurers reporting claims exceeding more than R140 million. The following categories of claims are reported:

- Unauthorised access to bank accounts – 68%.
- Unauthorised access to internal e-mail – 47%.
- Customer data being stolen – 46%.
- Systems locked with ransomware – 37%.

It is no defence for an attorney to claim they had the intention to pay the right person, but, due to fraud, they paid the wrong person. Practising attorneys are obliged to account to their clients for funds held in trust, and operate such accounts as principals. Fraudulent or negligent payment to the wrong person does not discharge the duties of an attorney to their clients.[52]

***Fourie v Van der Spuy and De Jongh Inc and others*[53]**

VDS was a law firm acting for F, its client. VDS received money that was due to be paid to F as the balance owing arising from a commercial transaction, and kept the money in its trust account. VDS then received a fraudulent e-mail instructing it to pay the full balance to a false bank account. Acting on the fraudulent e-mail, VDS drew the money from its trust account and paid it into the false bank account.

F demanded payment from VDS as he had not been paid. VDS requested F to make his laptop available for forensic testing to see if he had in fact sent the e-mail. However, F refused.

51 *Edcon Ltd v Cantamessa and others* [2020] 2 BLLR 186 (LC).

52 *Nissan South Africa (Pty) Ltd v Mamitz NO & others* 2005 (1) SA 441 (A); *Potgieter v Capricorn Beach Homeowners Association and another* (13667/2008) [2012] ZAWCHC 66 (20 March 2012); *Margalit v Standard Bank of South Africa and another* 2013 (2) SA 46 (SCA).

53 *Fourie v Van der Spuy and De Jongh Inc and others* 2020 (1) SA 560 (GP).

F sued VDS for payment; VDS claimed that it had at all times acted as a representative for F, and that he was therefore liable for the payment by VDS of the money from its trust account to the wrong bank account.

The court held that ownership of money in a trust account vests in the bank into which it has been deposited, and it is only the attorney who is entitled to operate the account and make withdrawals from it. When an attorney draws a cheque on their trust account, they do as principal, and not in a representative capacity. An attorney who holds money in a trust account on behalf of a client is obliged to use It for no other purpose than they are instructed. It is not a defence for the attorney to claim that they paid as they were instructed to do, when they did not verify the instructions.

To help deal with increased criminal activity online, Parliament passed the Cybercrimes Act.[54] The legislation creates several offences relating to hacking or unlawfully intercepting data or accessing a computer system or data storage medium, ransomware attacks, fraud, forgery, extortion, or theft of incorporeal property.

The Act also makes it a criminal offence to engage in 'malicious communications', which are data messages that incite damage to property or violence; threaten people with damage to property or violence; or disclose an intimate image. Penalties include imprisonment up to three years, and/or a fine of up to R50 000.

Electronic communications service providers and financial institutions must report certain offences within 72 hours. Failure to make the required report could lead to a fine of up to R50 000.

THIS CHAPTER IN ESSENCE

1 A domain name can create a lot of goodwill and can be very profitable. Profitability may be increased if a website uses a domain name with a respected or well-known trademark. A cybersquatter is someone who registers a domain name using another's trademark or other intellectual property and then attempts to sell the domain name to the proprietor.
2 Metatags are descriptive keywords that are inserted in the source code of websites to enable internet search engines to identify a particular site. Their value lies in their ability to optimise internet searches.
3 Intellectual property laws in nearly all countries prohibit downloading torrent files of copyright material.
4 Banner advertising occurs where an internet service provider hosting a website displays a large advertisement for goods, products or services at the top or on the side of the computer-screen image of the web page.
5 Contracts entered into over the internet have the same legal validity as any other contract. In terms of the Electronic Communication and Transactions Act it is possible for parties to enter into a valid contract by an electronic transaction. Contracts that by law must be in writing and which must be signed can be entered into electronically with certainty about enforceability. A data message can be incorporated by reference.
6 A contract is concluded at the place where and the time when a data message which contains the acceptance of an offer is received by the offeror.
7 The Electronic Communication and Transactions Act protects consumers who are natural persons by requiring vendors using websites for electronic transactions to provide 18 pieces of information.

54 Cybercrimes Act 19 of 2020.

8 Spam is the name given to unsolicited commercial communications.
9 As a general principle, defamation over the internet is regarded as having been committed where and when the defamatory material is accessed.
10 If an employer wishes to monitor internet and e-mail communications sent by its employees, a carefully worded internet and e-mail policy must be implemented and the consent of employees obtained.
11 Internet service providers that manage consumers' e-mail through their servers, as well as organisations that run their own e-mail servers, can be liable for negligence if they fail to adhere to the standard of care legally required of them.