REPUBLIC OF SOUTH AFRICA

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL

(As introduced in the National Assembly as a section 75 Bill; Bill published in Government Gazette No 23195 of 1 March 2002) (The English text is the official text of the Bill)

(MINISTER OF COMMUNICATIONS)

[B 8—2002]

ISBN 0 621 32099 4

No. of copies printed 1 500

BILL

To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:—

ARRANGEMENT OF SECTIONS

Sections

CHAPTER I

INTERPRETATION, OBJECTS AND APPLICATION

1. Definitions
2. Objects of Act
3. Interpretation
4. Sphere of application

CHAPTER II

MAXIMISING BENEFITS AND POLICY FRAMEWORK

Part 1

National e-strategy

5. National e-strategy
6. Universal access
7. Previously disadvantaged persons and communities
8. Development of human resources
9. SMMEs

Part 2

Electronic transactions policy

10. Electronic transactions policy

CHAPTER III

FACILITATING ELECTRONIC TRANSACTIONS

Part 1

Legal requirements for data messages

11. Legal recognition of data messages
12. Writing
13. Signature
14. Original
15. Admissibility and evidential weight of data messages
16. Retention
17. Production of document or information
18. Notarisation, acknowledgement and certification
19. Other requirements
20. Certain other legislation not affected
21. Automated transactions

Part 2

Communication of data messages

22. Variation by agreement between parties
23. Formation and validity of agreements
24. Time and place of communications, dispatch and receipt
25. Expression of intent or other statement
26. Attribution of data messages to originator
27. Acknowledgement of receipt of data message

CHAPTER IV

E-GOVERNMENT SERVICES

28. Acceptance of electronic filing and issuing of documents
29. Requirements may be specified

CHAPTER V

CRYPTOGRAPHY PROVIDERS

30. Register of cryptography providers
31. Registration with Department
32. Restrictions on disclosure of information
33. Application of Chapter and offences

CHAPTER VI

AUTHENTICATION SERVICE PROVIDERS

Part 1

Accreditation Authority

34. Definition
35. Appointment of Authority and other officers
36. Accreditation to be voluntary
37. Powers and duties of Authority

Part 2

Accreditation

38. Accreditation of authentication products and services
39. Criteria for accreditation
40. Revocation or termination of accreditation
41. Accreditation of foreign products and services
42. Accreditation regulations

CHAPTER VII

CONSUMER PROTECTION

43. Scope of application
44. Information to be provided
45. Cooling-off period
46. Unsolicited goods, services or communications
47. Performance
48. Applicability of foreign law
49. Non-exclusion
50. Complaints to Consumer Affairs Committee

CHAPTER VIII

PROTECTION OF PERSONAL INFORMATION

51. Scope of protection of personal information
52. Principles for electronically collecting personal information

CHAPTER IX

PROTECTION OF CRITICAL DATABASES

53. Scope of critical database protection
54. Identification of critical data and critical databases
55. Registration of critical databases
56. Management of critical databases
57. Restrictions on disclosure of information
58. Right of inspection
59. Non-compliance with Chapter

CHAPTER X

DOMAIN NAME AUTHORITY AND ADMINISTRATION

Part 1

Establishment and incorporation of Authority

60. Establishment of Authority
61. Incorporation of Authority
62. Authority's memorandum and articles of association

Part 2

Governance and staffing of Authority

63. Board of directors of Authority
64. Disqualification of directors
65. Remuneration and allowances of directors
66. Powers and duties of directors
67. Staff of Authority

Part 3

Functions of Authority

68. Licensing of registrars and registries
69. Functions of Authority

Part 4

Finances and reporting

70. Finances of Authority
71. Reports

Part 5

Regulations

72. Regulations regarding Authority

Part 6

Alternative dispute resolution

73. Alternative dispute resolution

CHAPTER XI

LIMITATION OF LIABILITY OF SERVICE PROVIDERS

74. Definition
75. Recognition of representative body
76. Conditions for eligibility
77. Mere conduit
78. Caching
79. Hosting
80. Information location tools
81. Take-down notification
82. No general obligation to monitor
83. Savings

CHAPTER XII

CYBER INSPECTORS

84. Appointment of cyber inspectors
85. Powers of cyber inspectors
86. Power to inspect, search and seize
87. Obtaining warrant
88. Preservation of confidentiality

CHAPTER XIII

CYBER CRIME

89. Definition
90. Unauthorised access to, interception of or interference with data
91. Computer-related extortion, fraud and forgery
92. Attempt, and aiding and abetting
93. Penalties

CHAPTER XIV

GENERAL PROVISIONS

94. Jurisdiction of courts
95. Saving of common law
96. Limitation of liability
97. Regulations
98. Short title and commencement

SCHEDULE 1

SCHEDULE 2

CHAPTER I

INTERPRETATION, OBJECTS AND APPLICATION

Definitions

1. In this Act, unless the context indicates otherwise—

"addressee", in respect of a data message, means a person who is intended by the originator to receive the data message, but not a person acting as an intermediary in respect of that data message;

"advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 38;

"authentication products or services" means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider" means a person whose authentication products or services have been accredited by the Authority under section 38 or recognised under section 41;

"Authority", for purposes of—

(a) Chapter VI, means the Director-General acting as the Accreditation Authority as provided for in that Chapter;

(b) Chapter X, means the .za Domain Name Authority established by that Chapter;

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment;

"browser" means a computer program which allows a person to read hyperlinked data messages;

"cache" means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing;

"ccTLD" means country code top level domain in the top level of the global domain name system assigned according to the two-letter codes in the International Standard ISO 3166-1 (Codes for Representation of Names of Countries and their Subdivision);

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message;

"consumer" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"Consumer Affairs Committee" means the Consumer Affairs Committee established by section 2 of the Consumer Affairs (Unfair Business Practices) Act, 1988 (Act No. 71 of 1988);

"critical data" means data that is declared by the Minister in terms of section 54 to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens;

"critical database" means a collection of critical data in electronic form from where it may be accessed, reproduced or retracted;

"critical database administrator" means the person responsible for the management and control of a critical database;

"cryptography product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—

(a) that such data can be accessed only by relevant persons;

(b) the authenticity of the data;

(c) the integrity of the data; or

(d) that the source of the data can be correctly ascertained;

"cryptography provider" means any person who provides or who proposes to provide cryptography services or products in the Republic;

"cryptography service" means any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—

(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;

(b) that the authenticity or integrity of such data or data message is capable of being ascertained;

(c) the integrity of the data or data message; or

(d) that the source of the data or data message can be correctly ascertained;

"cyber inspector" means an inspector referred to in Chapter XII;

"data" means electronic representations of information in any form;

"data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

"data message" means data generated, sent, received or stored by electronic means and includes—

(a) voice, where the voice is used in an automated transaction;

(b) a web page; and

(c) a stored record;

"data subject" means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

"Department" means the Department of Communications;

"Director-General" means the Director-General of the Department;

"domain name" means an alphanumeric designation that is registered or assigned in respect of an electronic address on the Internet;

"domain name system" means a system to translate domain names into IP addresses;

"e-government services" means any public service provided by electronic means by any public body in the Republic;

"electronic" means digital or other intangible form;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of data messages;

"electronic signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

"e-mail" means electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication;

"home page" means the primary entry point web page of a web site;

"hyperlink" means a reference or link from some point in one data message directing a browser or other technology or functionality to another data message or point therein or to another place in the same data message;

"ICANN" means the Internet Corporation for Assigned Names and Numbers, a California non-profit public benefit corporation established in terms of the laws of the state of California;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet and WAP communications;

"information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information

systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

"Internet" means an interconnected system of networks that connects computers around the world via TCP/IP and includes future versions thereof;

"IP address" means the unique set of alphanumerical characters identifying the location of a computer or data message on an information system or component part thereof;

"Minister" means the Minister of Communications;

"originator" means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;

"person" includes a public body;

"personal information" means information about an identifiable individual, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.

but excludes information about an individual who has been dead for more than 20 years;

"prescribe" means prescribe by regulation under this Act;

"private body" means—

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person,

but not a public body;

"public body" means—

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when—

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a power or performing a function in terms of any legislation;

"registrant" means an applicant for or holder of a domain name;

"registrar" means an entity which is licensed by the Authority to update a repository;

"registry" means an entity licensed by the Authority to manage and administer a specific subdomain;

"repository" means the primary register of the information maintained by a registry;
"second level domain" means the subdomain or subdomains immediately following the ccTLD, signifying a category or type of domain name;
"SMMEs" means Small, Medium and Micro Enterprises contemplated in the Schedules to the Small Business Development Act, 1996 (Act No. 102 of 1996);
"subdomain" means any subdivision of the .za domain name space which begins at the second level domain;
"TCP/IP" means the Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet;
"TLD" means the top level domain of the domain name system;
"third party", in relation to a service provider, means a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems;
"transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services;
"universal access" means access by all citizens of the Republic to Internet connectivity and electronic transactions;
"WAP" means Wireless Application Protocol, an open international standard developed by the Wireless Application Protocol Forum Limited, a company incorporated in terms of the laws of the United Kingdom, for applications that use wireless communication and includes Internet access from a mobile phone;
"web page" means a data message on the World Wide Web;
"web site" means any computer on the Internet containing a home page or web page;
"World Wide Web" means an Internet retrieval system for hyperlinked distributed information and includes all data messages residing on all computers linked to the Internet; and
".za domain name space" means the .za ccTLD assigned to the Republic according to the two-letter codes in the International Standard ISO 3166-1.

Objects of Act

2. (1) The objects of this Act are to enable and facilitate electronic transactions in the public interest, and for that purpose to—

(a) recognise the importance of the information economy to the future economic and social prosperity of the Republic;
(b) promote universal access;
(c) promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic;
(d) remove and prevent barriers to electronic transactions in the Republic;
(e) promote legal certainty and confidence in respect of electronic transactions;
(f) promote technology neutrality in the application of legislation to electronic transactions;
(g) promote e-government services and electronic transactions with public and private bodies and institutions;
(h) ensure that electronic transactions in the Republic conform to the highest international standards;
(i) encourage investment and innovation in respect of electronic transactions in the Republic;
(j) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;
(k) promote the development of electronic transactions services which are responsive to the needs of users and consumers;
(l) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities and, areas and the disabled are duly taken into account;
(m) ensure compliance with accepted technical standards in the provision and development of electronic transactions;
(n) promote the stability of electronic transactions in the Republic;
(o) promote the development of human resources in the electronic transactions environment;
(p) promote SMMEs within the electronic transactions environment;

(q) ensure efficient use and management of the .za domain name space; and
(r) ensure that the national interest of the Republic is not compromised through the use of electronic communications.

Interpretation

3. This Act must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act.

Sphere of application

4. (1) Subject to any contrary provision in this section, this Act applies in respect of any electronic transaction or data message.

(2) This Act must not be construed as—

(a) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form; or

(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

(3) The sections of this Act mentioned in Column B of Schedule 1 do not apply to the laws mentioned in Column A of that Schedule.

(4) This Act must not be construed as giving validity to any transaction mentioned in Schedule 2.

CHAPTER II

MAXIMISING BENEFITS AND POLICY FRAMEWORK

Part 1

National e-strategy

National e-strategy

5. (1) The Minister must, within 24 months after the promulgation of this Act, develop a five-year national e-strategy for the Republic, which must be submitted to the Cabinet for approval.

(2) The Cabinet must, on acceptance of the national e-strategy, declare the implementation of the national e-strategy as a national priority.

(3) The Minister, in developing the national e-strategy as envisaged in subsection (1)—

(a) must determine all matters involving e-government services in consultation with the Minister for the Public Service and Administration;

(b) must determine the roles and obligations of each person, entity or sector in the implementation of the national e-strategy;

(c) must act as the responsible Minister for co-ordinating and monitoring the implementation of the national e-strategy;

(d) may make such investigations as he or she may consider necessary;

(e) may conduct research into and keep abreast of developments relevant to electronic communications and transactions in the Republic and internationally;

(f) must continually survey and evaluate the extent to which the objectives of the national e-strategy have been achieved;

(g) may liaise, consult and cooperate with public bodies, the private sector or any other person; and

(h) may, in consultation with the Minister of Finance, appoint experts and other consultants on such conditions as the Minister may determine.

(4) (a) The Minister must, in consultation with other members of the Cabinet, determine the subject matters to be addressed in the national e-strategy and the principles that must govern the implementation thereof.

(b) Prior to prescribing any subject matter and principles provided for in paragraph *(a)*, the Minister must invite comments from all interested parties by notice in the *Gazette* and consider any comments received.

(c) The national e-strategy must, amongst others, set out—

(i) the electronic transactions strategy of the Republic, distinguishing between regional, national, continental and international strategies;

(ii) programmes and means to achieve universal access, human resource development and development of SMMEs as provided for in this Part;

(iii) programmes and means to promote the overall readiness of the Republic in respect of electronic transactions;

(iv) ways to promote the Republic as a preferred provider and user of electronic transactions in the international market;

(v) existing government initiatives directly or indirectly relevant to or impacting on the national e-strategy and, if applicable, how such initiatives are to be utilised in attaining the objectives of the national e-strategy;

(vi) the role expected to be performed by the private sector in the implementation of the national e-strategy and how government can solicit the participation of the private sector to perform such role;

(vii) the defined objectives, including time frames within which the objectives are to be achieved; and

(viii) the resources required to achieve the objectives provided for in the national e-strategy.

(5) Upon approval by the Cabinet, the Minister must publish the national e-strategy in the *Gazette*.

(6) For purposes of achieving the objectives of the national e-strategy, the Minister may, in consultation with the Minister of Finance—

(a) procure funding from sources other than the State;

(b) allocate funds for implementation of the national e-strategy to such institutions and persons as are responsible for delivery in terms of the national e-strategy and supervise the execution of their mandate; and

(c) take any steps necessary to enable all relevant parties to carry out their respective obligations.

(7) The Minister must annually report to the Cabinet on progress made and objectives achieved or outstanding and may include any other matter the Minister deems relevant.

(8) The Minister must annually review the national e-strategy and where necessary make amendments thereto in consultation with all relevant members of the Cabinet.

(9) No amendment or adaptation of the national e-strategy is effective unless approved by the Cabinet.

(10) The Minster must publish any material revision of the national e-strategy in the *Gazette*.

Universal access

6. In respect of universal access, the national e-strategy must outline strategies and programmes to—

(a) provide Internet connectivity to disadvantaged communities;

(b) encourage the private sector to initiate schemes to provide universal access;

(c) foster the adoption and use of new technologies for attaining universal access; and

(d) stimulate public awareness, understanding and acceptance of the benefits of Internet connectivity and electronic transacting.

Previously disadvantaged persons and communities

7. The Minister, in developing the national e-strategy, must provide for ways of maximising the benefits of electronic transactions to historically disadvantaged persons and communities, including, but not limited to—

(a) making facilities and infrastructure available or accessible to such persons and communities to enable the marketing and sale of their goods or services by way of electronic transactions;

(b) providing or securing support services for such facilities and infrastructure to assist with the efficient execution of electronic transactions; and

(c) rendering assistance and advice to such persons and communities on ways to adopt and utilise electronic transactions efficiently.

Development of human resources

8. (1) The Minister, in developing the national e-strategy, must provide for ways of promoting development of human resources set out in this section within the context of the government's integrated human resource development strategies, having regard to structures and programmes that have been established under existing laws.

(2) The Minister must consult with the Ministers of Labour and Education on existing facilities, programmes and structures for education, training and human resource development in the information technology sector relevant to the objects of this Act.

(3) Subject to subsections (1) and (2), the Minister must promote skills development in the areas of—

(a) information technology products and services in support of electronic transactions;
(b) business strategies for SMMEs and other businesses to utilise electronic transactions;
(c) sectoral, regional, national, continental and international policy formulation for electronic transactions;
(d) project management on public and private sector implementation of electronic transactions;
(e) the management of the .za domain name space;
(f) the management of the IP address system for the African continent in consultation with other African states;
(g) convergence between communication technologies affecting electronic transactions;
(h) technology and business standards for electronic transactions;
(i) education on the nature, scope, impact, operation, use and benefits of electronic transactions; and
(j) any other matter relevant to electronic transactions.

SMMEs

9. The Minister must, in consultation with the Minister of Trade and Industry, evaluate the adequacy of any existing processes, programmes and infrastructure providing for the utilisation by SMMEs of electronic transactions and, pursuant to such evaluation, may—

(a) establish or facilitate the establishment of electronic communication centres for SMMEs;
(b) facilitate the development of web sites or web site portals that will enable SMMEs to transact electronically and obtain information about markets, products and technical assistance; and
(c) facilitate the provision of such professional and expert assistance and advice to SMMEs on ways to utilise electronic transacting efficiently for their development.

Part 2

Electronic transactions policy

Electronic transactions policy

10. (1) The Minister must, subject to this Act, formulate electronic transactions policy.

(2) In formulating the policy contemplated in subsection (1), the Minister must—

(a) act in consultation with members of the Cabinet directly affected by such policy formulation or the consequences thereof;
(b) have due regard to—
  (i) the objects of this Act;
  (ii) the nature, scope and impact of electronic transactions;

(iii) international best practice and conformity with the law and guidelines of other jurisdictions and international bodies; and

(iv) existing laws and their administration in the Republic.

(3) The Minister must publish policy guidelines in the *Gazette* on issues relevant to electronic transactions in the Republic.

(4) The Minister may not publish policy guidelines that impose obligations on any person.

CHAPTER III

FACILITATING ELECTRONIC TRANSACTIONS

Part 1

Legal requirements for data messages

Legal recognition of data messages

11. (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.

(2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.

(3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is—

(a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and

(b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

Writing

12. A requirement in law that a document or information must be in writing is met if the document or information is—

(a) in the form of a data message; and

(b) accessible in a manner usable for subsequent reference.

Signature

13. (1) Where the signature of a person is required by law, that requirement in relation to a data message is met only if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if—

(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and

(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

(4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Subsection (4) does not preclude any person from—

(a) establishing the validity of an advanced electronic signature in any other way; or

(b) adducing evidence of the non-validity of an advanced electronic signature.

Original

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if—

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1*(a)*, the integrity must be assessed—

(a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

Admissibility and evidential weight of data messages

15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence—

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

Retention

16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if—

(a) the information contained in the data message is accessible so as to be usable for subsequent reference;

(b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Production of document or information

17. (1) Subject to section 29, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if—

(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for—

(a) the addition of any endorsement; or

(*b*) any immaterial change, which arises in the normal course of communication, storage or display.

Notarisation, acknowledgement and certification

18. (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

Other requirements

19. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

Certain other legislation not affected

20. This Act does not limit the operation of any law that expressly authorises, prohibits or regulates the use of data messages, including any requirement by or under a law for information to be posted or displayed in a specified manner, or for any information or document to be transmitted by a specified method.

Automated transactions

21. In an automated transaction—

(*a*) an agreement may be formed where an electronic agent performs an action required by law for agreement formation;

(*b*) an agreement may be formed where all parties to a transaction or either one of them uses an electronic agent;

(*c*) a party using an electronic agent to form an agreement is, subject to paragraph (*d*), bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement;

(*d*) a party using an electronic agent to form an agreement is not bound by the terms of that agreement unless those terms were capable of being reviewed by a natural person prior to agreement formation;

(*e*) no agreement is formed where a natural person interacts directly with the electronic agent of another person and has made a material error during the creation of a data message and—

(i) the electronic agent did not provide that person with an opportunity to prevent or correct the error;

(ii) that person notifies the other person of the error as soon as practicable after that person has learned of it;

(iii) that person takes reasonable steps, including steps that conform to the other person's instructions to return any performance received, or, if instructed to do so, to destroy that performance; and

(iv) that person has not used or received any material benefit or value from any performance received from the other person.

Part 2

Communication of data messages

Variation by agreement between parties

22. This Part only applies if the parties involved in generating, sending, receiving, storing or otherwise processing data messages have not reached agreement on the issues provided for therein.

Formation and validity of agreements

23. (1) An agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages.

(2) An agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offeror.

Time and place of communications, dispatch and receipt

24. A data message—

(a) used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee;

(b) must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee; and

(c) must be regarded as having been sent from the originator's usual place of business and as having been received at the addressee's usual place of business.

Expression of intent or other statement

25. As between the originator and the addressee of a data message an expression of intent or other statement is not without legal force and effect merely on the grounds that—

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but by other means from which such person's intent or other statement can be inferred.

Attribution of data messages to originator

26. A data message is that of the originator if it was sent by—

(a) the originator personally;

(b) a person who had authority to act on behalf of the originator in respect of that data message; or

(c) an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgement of receipt of data message

27. (1) An acknowledgement of receipt of a data message is not necessary to give legal effect to that message.

(2) An acknowledgement of receipt may be given by—

(a) any communication by the addressee, whether automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

CHAPTER IV

E-GOVERNMENT SERVICES

Acceptance of electronic filing and issuing of documents

28. Any public body that, pursuant to any law—

(a) accepts the filing of documents, or requires that documents be created or retained;

(b) issues any permit, licence or approval; or

(c) provides for a manner of payment,

may, notwithstanding anything to the contrary in such law—

(i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages;

(ii) issue such permit, licence or approval in the form of a data message; or

(iii) make or receive payment in electronic form or by electronic means.

Requirements may be specified

29. In any case where a public body performs any of the functions referred to in section 28, such body may specify by notice in the *Gazette*—

(a) the manner and format in which the data messages must be filed, created, retained or issued;

(b) in cases where the data message has to be signed, the type of electronic signature required;

(c) the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message;

(d) the identity of or criteria that must be met by any authentication service provider used by the person filing the data message;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(f) any other requirements for data messages or payments.

CHAPTER V

CRYPTOGRAPHY PROVIDERS

Register of cryptography providers

30. (1) The Director-General must establish and maintain a register of cryptography providers.

(2) The Director-General must record the following particulars in respect of a cryptography provider in that register:

(a) The name and address of the cryptography provider;

(b) a description of the type of cryptography service or cryptography product being provided; and

(c) such other particulars as may be prescribed to identify and locate the cryptography provider or its products or services adequately.

(3) A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.

Registration with Department

31. (1) No person may provide cryptography services or cryptography products in the Republic until the particulars referred to in section 30(2) in respect of that person have been recorded in the register contemplated in section 30(1).

(2) A cryptography provider must in the prescribed manner furnish the Director-General with the information required and pay the prescribed administrative fee.

(3) A cryptography service or cryptography product is regarded as being provided in the Republic if it is provided—

(a) from premises in the Republic;

(b) to a person who is present in the Republic when that person makes use of the service or product; or

(c) to a person who uses the service or product for the purposes of a business carried on in the Republic or from premises in the Republic.

Restrictions on disclosure of information

32. (1) Information contained in the register provided for in section 30 must not be disclosed to any person other than to employees of the Department who are responsible for the keeping of the register.

(2) Subsection (1) does not apply in respect of information which is disclosed—

(a) to a relevant authority which investigates a criminal offence or for the purposes of any criminal proceedings;

(b) to government agencies responsible for safety and security in the Republic, pursuant to an official request;

(c) to a cyber inspector;

(d) pursuant to section 11 or 30 of the Promotion of Access to Information Act, (Act No. 2 of 2000); or

(e) for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

Application of Chapter and offences

33. (1) The provisions of this Chapter do not apply to the National Intelligence Agency established in terms of section 3 of the Intelligence Services Act, 1994 (Act No. 38 of 1994).

(2) A person who contravenes or fails to comply with a provision of this Chapter is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.

CHAPTER VI

AUTHENTICATION SERVICE PROVIDERS

Part 1

Accreditation Authority

Definition

34. In this Chapter, unless the context indicates otherwise—

"accreditation" means recognition of an authentication product or service by the Authority.

Appointment of Authority and other officers

35. (1) For the purposes of this Chapter the Director-General must act as the Authority.

(2) The Authority, after consultation with the Minister, may appoint employees of the Department as Deputy Authorities and officers.

Accreditation to be voluntary

36. Subject to section 31(1), a person may, without the prior authority of any other person, sell or provide authentication products or services in the Republic.

Powers and duties of Authority

37. (1) The Authority may—

(a) monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 39 and the other obligations of authentication service providers in terms of this Act;

(b) temporarily suspend or revoke the accreditation of an authentication product or service; and

(c) appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 39 and the other obligations of authentication service providers in terms of this Act.

(2) The Authority must maintain a publicly accessible database in respect of—

(a) authentication products or services accredited in terms of section 38;
(b) authentication products and services recognised in terms of section 41;
(c) revoked accreditations or recognitions; and
(d) such other information as may be prescribed.

Part 2

Accreditation

Accreditation of authentication products and services

38. (1) The Authority may accredit authentication products and services in support of advanced electronic signatures.

(2) An application for accreditation must—

(a) be made to the Authority in the prescribed manner supported by the prescribed information; and
(b) be accompanied by a non-refundable prescribed fee.

(3) A person falsely holding out its products or services to be accredited by the Authority is guilty of an offence.

Criteria for accreditation

39. (1) The Authority may not accredit authentication products or services unless the Authority is satisfied that an electronic signature to which such authentication products or services relate—

(a) is uniquely linked to the user;
(b) is capable of identifying that user;
(c) is created using means that can be maintained under the sole control of that user; and
(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable.

(2) For purposes of subsection (1), the Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services:

(a) Its financial and human resources, including its assets;
(b) the quality of its hardware and software systems;
(c) its procedures for processing of products or services;
(d) the availability of information to third parties relying on the authentication product or service;
(e) the regularity and extent of audits by an independent body;
(f) the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and
(g) any other relevant factor which may be prescribed.

(3) For the purposes of subsections (2)(b) and (c), the hardware and software systems and procedures must at least—

(a) be reasonably secure from intrusion and misuse;
(b) provide a reasonable level of availability, reliability and correct operation;
(c) be reasonably suited to performing their intended functions; and
(d) adhere to generally accepted security procedures.

(4) For the purposes of subsection (1), where the products or services are provided by a certification service provider, the Authority may stipulate, prior to accrediting authentication products or services—

(a) the technical and other requirements which certificates must meet;
(b) the requirements for issuing certificates;
(c) the requirements for certification practice statements;
(d) the responsibilities of the certification service provider;
(e) the liability of the certification service provider;
(f) the records to be kept and the manner in which and length of time for which they must be kept;

(g) requirements as to adequate certificate suspension and revocation procedures; and

(h) requirements as to adequate notification procedures relating to certificate suspension and revocation.

(5) The Authority may impose any conditions or restrictions necessary when accrediting an authentication product or service.

Revocation or termination of accreditation

40. (1) The Authority may suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 39 or recognition was given in terms of section 41.

(2) Subject to the provisions of subsection (3), the Authority may not suspend or revoke the accreditation or recognition contemplated in subsection (1) unless it has—

(a) notified the authentication service provider in writing of its intention to do so;

(b) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted under section 39 or recognition was given in terms of section 41; and

(c) afforded the authentication service provider the opportunity to—

(i) respond to the allegations in writing; and

(ii) remedy the alleged breach within a reasonable time.

(3) The Authority may suspend accreditation granted under section 39 or recognition given under section 41 with immediate effect for a period not exceeding 90 days, pending implementation of the procedures required by subsection (2), if the continued accreditation or recognition of the authentication service provider is reasonably likely to result in irreparable harm to consumers or any person involved in an electronic transaction in the Republic.

(4) An authentication service provider whose products or services have been accredited in terms of this Chapter may terminate such accreditation at any time, subject to such conditions as may be agreed to at the time of accreditation or thereafter.

Accreditation of foreign products and services

41. (1) The Minister may, by notice in the *Gazette* and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.

(2) An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1), is guilty of an offence.

Accreditation regulations

42. The Minister may make regulations in respect of—

(a) the rights and obligations of persons relating to the provision of accredited products and services;

(b) the manner in which the Authority must administer and supervise compliance with those obligations;

(c) the procedure pertaining to the granting, suspension and revocation of accreditation;

(d) fees to be paid;

(e) information security requirements or guidelines; and

(f) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Chapter.

CHAPTER VII

CONSUMER PROTECTION

Scope of application

43. (1) This Chapter applies only to electronic transactions.

(2) Section 45 does not apply to an electronic transaction—

(a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;
(b) by way of an auction;
(c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;
(d) for services which began with the consumer's consent before the end of the seven-day period referred to in section 45(1);
(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;
(f) where the goods—
(i) are made to the consumer's specifications;
(ii) are clearly personalised;
(iii) by reason of their nature cannot be returned; or
(iv) are likely to deteriorate or expire rapidly;
(g) where audio or video recordings or computer software were unsealed by the consumer;
(h) for the sale of newspapers, periodicals and magazines;
(i) for the provision of gaming and lottery services; or
(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

Information to be provided

44. (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make the following information available to consumers on the web site where such goods or services are offered:
(a) Its full name and legal status;
(b) its physical address and telephone number;
(c) its web site address and e-mail address;
(d) membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body;
(e) any code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;
(f) in the case of a legal person, its registration number, the names of its office bearers and its place of registration;
(g) the physical address where that supplier will receive legal service of documents;
(h) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;
(i) the full price of the goods or services, including transport costs, taxes and any other fees or costs;
(j) the manner of payment;
(k) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;
(l) the time within which the goods will be dispatched or delivered or within which the services will be rendered;
(m) the manner and period within which consumers can access and maintain a full record of the transaction;
(n) the return, exchange and refund policy of that supplier;
(o) any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer;
(p) the security procedures and privacy policy of that supplier in respect of payment, payment information and personal information;
(q) where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently; and
(r) the rights of consumers in terms of section 45, where applicable.

(2) The supplier must provide a consumer with an opportunity—

(*a*) to review the entire electronic transaction;
(*b*) to correct any mistakes; and
(*c*) to withdraw from the transaction, before finally placing any order.

(3) If a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.

(4) If a transaction is cancelled in terms of subsection (3)—
(*a*) the consumer must return the performance of the supplier or, where applicable, cease using the services performed; and
(*b*) the supplier must refund all payments made by the consumer minus the direct cost of returning the goods.

(5) The supplier must utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

Cooling-off period

45. (1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply—
(*a*) of goods within seven days after the date of the receipt of the goods; or
(*b*) of services within seven days after the date of the conclusion of the agreement.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment, which refund must be made within 30 days of the date of cancellation.

(4) This section must not be construed as prejudicing the rights of a consumer provided for in any other law.

Unsolicited goods, services or communications

46. (1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer—
(*a*) with the option to cancel his or her subscription to the mailing list of that person; and
(*b*) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

Performance

47. (1) The supplier must execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise .

(2) Where a supplier has failed to execute the order within 30 days or within the agreed period, the consumer may cancel the agreement with seven days' written notice.

(3) If a supplier is unable to perform in terms of the agreement on the grounds that the goods or services ordered are unavailable, the supplier must immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification.

Applicability of foreign law

48. The protection provided to consumers in this Chapter, applies irrespective of the legal system applicable to the agreement in question.

Non-exclusion

49. Any provision in an agreement which excludes any rights provided for in this Chapter is null and void.

Complaints to Consumer Affairs Committee

50. A consumer may lodge a complaint with the Consumer Affairs Committee in respect of any non-compliance with the provisions of this Chapter by a supplier.

CHAPTER VIII

PROTECTION OF PERSONAL INFORMATION

Scope of protection of personal information

51. (1) This Chapter only applies to personal information that has been obtained through electronic transactions.

(2) A data controller may voluntarily subscribe to the principles outlined in section 52 by recording such fact in any agreement with a data subject.

(3) A data controller must subscribe to all the principles outlined in section 52 and not merely to parts thereof.

(4) The rights and obligations of the parties in respect of the breach of the principles outlined in section 52 are governed by the terms of any agreement between them.

Principles for electronically collecting personal information

52. (1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

(2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.

(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.

(8) The data controller must delete or destroy all personal information which has become obsolete.

(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

CHAPTER IX

PROTECTION OF CRITICAL DATABASES

Scope of critical database protection

53. The provisions of this Chapter only apply to a critical database administrator and critical databases or parts thereof.

Identification of critical data and critical databases

54. The Minister may by notice in the *Gazette*—

(a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data for the purposes of this Chapter; and

(b) establish procedures to be followed in the identification of critical databases for the purposes of this Chapter.

Registration of critical databases

55. (1) The Minister may by notice in the *Gazette* determine—

(a) requirements for the registration of critical databases with the Department or such other body as the Minister may specify;

(b) procedures to be followed for registration; and

(c) any other matter relating to registration.

(2) For purposes of this Chapter, registration of a critical database means recording the following information in a register maintained by the Department or by such other body as the Minister may specify:

(a) The full name, address and contact details of the critical database administrator;

(b) the location of the critical database, including the locations of component parts thereof where a critical database is not stored at a single location; and

(c) a general description of the categories or types of information stored in the critical database.

Management of critical databases

56. (1) The Minister may prescribe minimum standards or prohibitions in respect of—

(a) the general management of critical databases;

(b) access to, transfer and control of critical databases;

(c) infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical data;

(d) procedures and technological methods to be used in the storage or archiving of critical databases;

(e) disaster recovery plans in the event of loss of critical databases or parts thereof; and

(f) any other matter required for the adequate protection, management and control of critical databases.

(2) In respect of critical databases administered by public bodies, all regulations contemplated in subsection (1) must be made in consultation with all members of the Cabinet affected by the provisions of this Chapter: Provided that the Minister must not record information contemplated in section 55(2) if that information could reasonably compromise—

(a) the security of such databases; or

(b) the physical safety of a person in control of the critical database.

(3) This Chapter must not be construed so as to prejudice the right of a public body to perform any function authorised in terms of any other law.

Restrictions on disclosure of information

57. (1) Information contained in the register provided for in section 55 must not be disclosed to any person other than to employees of the Department who are responsible for the keeping of the register.

(2) Subsection (1) does not apply in respect of information which is disclosed—

(a) to a relevant authority which is investigating a criminal offence or for the purposes of any criminal proceedings;

(b) to government agencies responsible for safety and security in the Republic pursuant to an official request;

(c) to a cyber inspector for purposes of section 58;

(d) pursuant to sections 11 and 30 of the Promotion of Access to Information Act, 2000; or

(e) for the purposes of any civil proceedings which relate to the critical data or parts thereof.

Right of inspection

58. (1) The Director-General may, from time to time, cause audits to be performed at a critical database administrator to evaluate compliance with the provisions of this Chapter.

(2) The audit may be performed either by cyber inspectors or an independent auditor.

Non-compliance with Chapter

59. (1) Should the audit contemplated in section 58 reveal non-compliance by the critical database administrator with this Chapter, the Director-General must notify the critical database administrator thereof in writing, stating—

(a) the finding of the audit report;

(b) the action required to remedy the non-compliance; and

(c) the period within which the remedial action must be performed.

(2) A critical database administrator that fails to take the remedial action within the period stated in the notice is guilty of an offence.

CHAPTER X

DOMAIN NAME AUTHORITY AND ADMINISTRATION

Part 1

Establishment and incorporation of Authority

Establishment of Authority

60. A juristic person to be known as the .za Domain Name Authority is hereby established for the purpose of assuming responsibility for the .za domain name space as from a date determined by the Minister by notice in the *Gazette*.

Incorporation of Authority

61. (1) The Minister must, within 12 months of the date of commencement of this Act, take all steps necessary for the incorporation of the Authority as a company contemplated in section 21(1) of the Companies Act, 1973 (Act No. 61 of 1973).

(2) Despite the provisions of the Companies Act, 1973, the State will be the only member and shareholder of the Authority upon its incorporation and at any time thereafter.

(3) The State's rights as member and shareholder of the Authority must be exercised by the Minister.

Authority's memorandum and articles of association

62. (1) The memorandum of association and articles of association of the Authority must be consistent with this Chapter.

(2) Notwithstanding the Companies Act, 1973, an amendment to the memorandum of association or articles of association affecting any arrangement made by any provision of this Chapter, does not have any legal force and effect unless the Minister has consented in writing to such an amendment.

(3) No fee is payable in terms of the Companies Act, 1973, in respect of the reservation of the name of the company, the registration of the said memorandum and articles and the issue of the certificate to commence business.

(4) The memorandum and articles of association of the Authority must, amongst others, provide for—

(a) the rules for the convening and conducting of meetings of the Board, including the quorum required for and the minutes to be kept of those meetings;

(b) the manner in which decisions are to be made;

(c) the establishment of any division of the Authority to perform specialised functions;

(d) the establishment and functioning of committees, including a management committee;

(e) the co-opting by the Board or a committee of any person to assist the Authority or committee in the consideration of any particular matter;

(f) the preparation by the Board, for approval by the Minister, of an annual business plan in terms of which the activities of the Authority are planned annually;

(g) the banking and investment of funds by the Board;

(h) provisions to regulate the manner in which, and procedures whereby, expertise from any person is obtained in order to further the objects of the Authority;

(i) the determination through arbitration of any dispute concerning the interpretation of the memorandum and articles of association of the Authority; and

(j) the delegation of powers and assignment of duties to directors, committees and employees: Provided that the Board may—

(i) not be divested of any power or duty by virtue of the delegation or assignment; and

(ii) vary or set aside any decision made under any delegation or in terms of any assignment.

Part 2

Governance and staffing of Authority

Board of directors of Authority

63. (1) The Authority is managed and controlled by a board of directors consisting of no fewer than eight, and no more than 16 persons, appointed by the Minister.

(2) *(a)* The Minister must, by notice in the *Gazette* and in two newspapers which have general circulation throughout the Republic, invite the stakeholders mentioned in paragraph *(b)* to nominate two persons to serve as directors on the Board of the Authority and one person to act as an alternate director to the Board.

(b) The stakeholders contemplated in paragraph *(a)* are—

(i) the Internet community;

(ii) the business community;

(iii) academic institutions and institutions of higher learning;

(iv) non-governmental organisations;

(v) government and the public service sector;

(vi) the disabled;

(vii) SMMEs; and

(viii) civil society comprised of persons not falling within any of the aforementioned categories.

(3) Directors must be persons who are committed to fairness, openness and accountability and to the objects of this Act.

(4) When viewed collectively the Board must be broadly representative of the demographics of the Republic.

(5) The Minister may, in terms of the criteria referred to in subsections (3) and (4), appoint persons—

(a) other than those nominated, if a sufficient number of persons who meet the criteria are not nominated; or

(b) if there are insufficient nominations lodged within the period specified in the notice.

(6) *(a)* The Minister must determine—

(i) the tenure of the directors; and

(ii) the circumstances under and manner in which a directorship is terminated; and

(iii) the procedures for the replacement of such directors.

(b) The matters determined by the Minister in terms of paragraph *(a)*(i) and (ii) must be contained in the letter of appointment to be handed to each director on appointment.

(c) The Minister must by notice in the *Gazette* publish the matters determined in terms of paragraph *(a)*(iii).

(7) All directors serve in a part-time and non-executive capacity.

Disqualification of directors

64. (1) A person may not be appointed or continue to serve as a director if such a person—

(a) is not a citizen of the Republic;
(b) is not permanently resident in the Republic;
(c) repeatedly fails to perform the duties of that office efficiently;
(d) is guilty of misconduct;
(e) because of any physical or mental illness, has become incapable of performing the functions of that office efficiently; or
(f) is disqualified from being appointed as a director of a company in the Republic.

(2) A person who is subject to a disqualification contemplated in this section may be nominated for appointment, and may be appointed as a director of the Board, if, at the time of such appointment, he or she is no longer subject to that disqualification.

Remuneration and allowances of directors

65. (1) The Minister must, in consultation with the Minister of Finance, determine the remuneration and allowances of directors and alternate directors of the Board.

(2) Persons referred to in subsection (1) who are in the service of the State may not receive additional remuneration or allowances for serving on the Board, but may be reimbursed for expenses incurred in the performance of their functions in serving on the Board.

Powers and duties of directors

66. The directors must administer the Authority in accordance with its functions in terms of this Act and have the powers and duties normally accorded to a board of directors in terms of the Companies Act, 1973.

Staff of Authority

67. (1) The chief executive officer of the Authority appointed by the Board must perform any work incidental to the functions of the Authority.

(2) The chief executive officer must be assisted by staff appointed by the Board.

(3) The Board must determine the conditions of service, remuneration and service benefits of the chief executive officer and the staff.

(4) If the chief executive officer is for any reason unable to perform his or her functions, the Board may designate a person in the service of the Authority to act as the chief executive officer until the chief executive officer is able to resume office.

Part 3

Functions of Authority

Licensing of registrars and registries

68. (1) No person may update a repository or administer a subdomain unless such person is licensed to do so by the Authority.

(2) An application to be licensed as a registrar or registry must be made in the prescribed manner and subject to the prescribed fees.

(3) The Authority must apply the prescribed conditions and criteria when evaluating an application referred to in subsection (2).

Functions of Authority

69. (1) The Authority must—

(a) administer and manage the .za domain name space;
(b) comply with the requirements for administration of the .za domain name space as provided for by ICANN, its successors or assigns;
(c) license and regulate registries;
(d) license and regulate registrars for the respective registries; and

(e) publish guidelines on—

(i) the general administration and management of the .za domain name space;

(ii) the requirements and procedures for domain name registration; and

(iii) the maintenance of and public access to a repository, with due regard to the policy directives which the Minister may make from time to time by notice in the *Gazette*.

(2) The Authority must enhance public awareness of the economic and commercial benefits of domain name registration.

(3) The Authority—

(a) may conduct such investigations as it may consider necessary;

(b) must conduct research into and keep abreast of developments in the Republic and elsewhere on the domain name system;

(c) must continually survey and evaluate the extent to which the .za domain name space meets the needs of the citizens of the Republic; and

(d) may, from time to time, issue information on the registration of domain names in the Republic.

(4) The Authority may, and must when so requested by the Minister, make recommendations to the Minister in relation to policy on any matter relating to the .za domain name space.

(5) The Authority must continually evaluate the effectiveness of this Act and things done in terms thereof towards the management of the .za domain name space.

(6) The Authority may—

(a) liaise, consult and co-operate with any person or other authority; and

(b) appoint experts and other consultants on such conditions as the Authority may determine.

(7) The Authority must respect and uphold the vested rights and interests of parties that were actively involved in the management and administration of the .za domain name space at the date of its establishment: Provided that—

(a) such parties must be granted a period of six months during which they may continue to operate in respect of their existing delegated subdomains;

(b) after the expiry of the six-month period, such parties must duly apply to be licensed registrars and registries as provided for in this Part.

Part 4

Finances and reporting

Finances of Authority

70. (1) All money received by the Authority must be deposited in a banking account in the name of the Authority with a bank established under the Banks Act, 1990 (Act No. 94 of 1990), or a mutual bank established under the Mutual Banks Act, 1993 (Act No. 124 of 1993).

(2) The financial year of the Authority begins on 1 July and ends on 30 June of the following year.

(3) The chief executive officer is the accounting officer of the Authority and must ensure that—

(a) proper record of all the financial transactions, assets and liabilities of the Authority is kept; and

(b) as soon as possible, but not later than three months after the end of a financial year, accounts reflecting the income and expenditure of the Authority and a balance sheet of the assets and liabilities of the Authority as at the end of that financial year are prepared and submitted to the Board and Minister.

(4) The Authority is funded from—

(a) the capital invested in or lent to the Authority;

(b) money appropriated by Parliament for that purpose;

(c) income derived from the sale or other commercial exploitation of its licenses, approvals, products, technology, services or expertise in terms of this Act:

(d) loans raised by the Authority;

(e) the proceeds of any sale of assets;

(f) income or interest earned on the Authority's cash balances or on money invested by it; and

(g) money received by way of grant, contribution, donation or inheritance from any source inside or outside the Republic.

(5) The funds of the Authority must be utilised to meet the expenditure incurred by the Authority in connection with its functioning, business and operations in terms of this Act.

(6) *(a)* The money may be so utilised only as provided for in a statement of the Authority's estimated income and expenditure contemplated in subsection (4) that has been approved by the Minister.

(b) Money received by way of grant, contribution, donation or inheritance in terms of subsection (4)*(g)*, must be utilised in accordance with any conditions imposed by the grantor, contributor, donor or testator concerned.

(7) *(a)* The Board must in each financial year, at a time determined by the Minister, submit to the Minister for approval a statement of the Authority's estimated income and expenditure for the next financial year.

(b) The Board may at any time during the course of a financial year submit a supplementary statement of estimated income and expenditure of the Authority for that financial year to the Minister for approval.

(c) The Minister may grant the approval of the statement referred to in paragraph *(a)*, with the agreement of the Minister of Finance.

(d) The Authority may not incur any expenditure in excess of the total amount approved under paragraph *(c)*.

(8) The Board may establish a reserve fund for any purpose that is connected with the Authority's functions under this Act and has been approved by the Minister, and may allocate to the reserve fund the money that may be made available for that purpose in the statement of estimated income and expenditure or supplementary statement contemplated in subsection (7).

(9) To the extent that the Authority is provided with start-up capital by the State, the Authority may, at the election of the Minister of Finance, be made subject to the Public Finance Management Act, (Act No. 1 of 1999), until such time as the Authority, to the satisfaction of the Minister of Finance, becomes self-sustaining through the alternative sources of revenue provided for in subsection (4).

Reports

71. As soon as practicable after the end of each financial year, the Board must submit a report on its activities during that year to the Minister.

Part 5

Regulations

Regulations regarding Authority

72. The Minister may make regulations regarding—

(a) the requirements which registries and registrars must meet in order to be licensed, including objective standards relating to operational accuracy, stability, robustness and efficiency;

(b) the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries with due regard to the express recognition of the right of groups and members of groups within the Republic to identify with, use or communicate cultural, linguistic, geographical, indigenous or any other expressions of heritage including any visual or audible elements or attributes thereof;

(c) pricing policy;

(d) provisions for the restoration of a domain name registration and penalties for late payments;

(e) the terms of the domain name registration agreement which registries and registrars must adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution;

(f) processes and procedures to avoid unfair and anti-competitive practices, including bias to, or preferential treatment of, actual or prospective registrants, registries or registrars, protocols or products;

(g) requirements to ensure that each domain name contains an administrative and technical contact;
(h) the creation of new subdomains;
(i) procedures for ensuring monitoring of compliance with the provisions of this Act and the regulations provided for in this Chapter, including regular .za domain name space technical audits;
(j) such other matters relating to the .za domain name space as it may be necessary to prescribe to achieve the objectives of this Chapter; and
(k) policy to be applied by the Authority.

Part 6

Alternative dispute resolution

Alternative dispute resolution

73. (1) The Minister, in consultation with the Minister for Trade and Industry, must make regulations for an alternative mechanism for the resolution of disputes in respect of the .za domain name space.

(2) The regulations must be made with due regard to existing international precedent.

(3) The regulations may prescribe—

(a) dispute-resolution procedures in the event of a dispute relating to a domain name registration;
(b) the role which the Authority must fulfil in administering the dispute-resolution procedure;
(c) the appointment, role and function of dispute-resolution adjudicators;
(d) the procedure and rules which must be followed in adjudicating disputes;
(e) unlawful actions or activities in respect of domain names, distinguishing between criminal and civil liability;
(f) measures to prevent unlawful actions or activities with respect to domain names;
(g) the costs of a determination, and the manner in which and time within which a determination must be made;
(h) the implementation of determinations made in terms of the dispute-resolution procedure;
(i) the limitation of liability of registrars and registries for implementing a determination; and
(j) the enforcement and publication of determinations.

CHAPTER XI

LIMITATION OF LIABILITY OF SERVICE PROVIDERS

Definition

74. In this Chapter, "service provider" means any person providing information system services.

Recognition of representative body

75. (1) The Minister may, on application by an industry representative body for service providers by notice in the *Gazette*, recognise such body for purposes of section 76.

(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister is satisfied that—

(a) its members are subject to a code of conduct;
(b) membership is subject to adequate criteria;
(c) the code of conduct requires continued adherence to adequate standards of conduct; and
(d) the representative body is capable of monitoring and enforcing its code of conduct adequately.

Conditions for eligibility

76. The limitations on liability established by this Chapter apply to a service provider only if—

(a) the service provider is a member of the representative body referred to in section 75; and

(b) the service provider has adopted and implemented the official code of conduct of that representative body.

Mere conduit

77. (1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider—

(a) does not initiate the transmission;

(b) does not select the addressee;

(c) performs the functions in an automatic, technical manner without selection of the data; and

(d) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place—

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and

(c) for a period no longer than is reasonably necessary for the transmission.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

Caching

78. (1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—

(a) does not modify the data;

(b) complies with conditions on access to the data;

(c) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by industry;

(d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain information on the use of the data; and

(e) removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 81.

(2) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

Hosting

79. (1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider—

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and

(c) upon receipt of a take-down notification referred to in section 81, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its web sites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

(4) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

Information location tools

80. A service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider—

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to such data message, infringes the rights of a person.

Take-down notification

81. For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include—

(a) the full names and address of the complainant;

(b) the written or electronic signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith;

(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and

(i) an undertaking given by the complainant to indemnify the service provider from any liability incurred as a result of remedial action taken by it in complying with the notification.

No general obligation to monitor

82. (1) When providing the services contemplated in this Chapter there is no a general obligation on a service provider to—

(a) monitor the data which it transmits or stores; or

(b) actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to section 14 of the Constitution, prescribe procedures for service providers to—

(a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

(b) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

Savings

83. This Chapter does not affect—

(a) any obligation founded on an agreement;

(b) the obligation of a service provider acting as such under a licensing or other regulatory regime established by or under any law; or

(c) any obligation imposed by law or by a court to remove, block or deny access to any data message.

CHAPTER XII

CYBER INSPECTORS

Appointment of cyber inspectors

84. (1) The Director-General may appoint any employee of the Department as a cyber inspector empowered to perform the functions provided for in this Chapter.

(2) A cyber inspector must be provided with a certificate of appointment signed by or on behalf of the Director-General in which it is stated that he or she has been appointed as a cyber inspector.

(3) A certificate provided for in subsection (2) may be in the form of an advanced electronic signature.

(4) When a cyber inspector performs any function in terms of this Act, he or she must—

(a) be in possession of a certificate of appointment referred to in subsection (2); and

(b) show that certificate to any person who—

(i) is subject to an investigation or an employee of that person; or

(ii) requests to see the certificate.

(5) Any person who—

(a) hinders or obstructs a cyber inspector in the performance of his or her functions in terms of this Chapter; or

(b) falsely holds himself or herself out as a cyber inspector.

is guilty of an offence.

Powers of cyber inspectors

85. (1) A cyber inspector may—

(a) monitor and inspect any web site or activity on an information system in the public domain and report any unlawful activity to the appropriate authority;

(b) in respect of a cryptography service provider—

(i) investigate the activities of a cryptography service provider in relation to its compliance or non-compliance with the provisions of this Act; and

(ii) issue an order in writing to a cryptography service provider to comply with the provisions of this Act;

(c) in respect of an authentication service provider—

(i) investigate the activities of an authentication service provider in relation to its compliance or non-compliance with the provisions of this Act;

(ii) investigate the activities of an authentication service provider falsely holding itself, its products or services out as having been accredited by the Authority or recognised by the Minister as provided for in Chapter VI;

(iii) issue an order in writing to an authentication service provider to comply with the provisions of this Act; and

(d) in respect of a critical database administrator, perform an audit as provided for in section 58.

(2) Any statutory body, including the South African Police Service, with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector to assist it in an investigation: Provided that—

(a) the requesting body must apply to the Department for assistance in the prescribed manner; and

(b) the Department may authorise such assistance on certain conditions.

Power to inspect, search and seize

86. (1) A cyber inspector may, in the performance of his or her functions, at any reasonable time, without prior notice and on the authority of a warrant issued in terms of section 87(1), enter any premises or access an information system that has a bearing on an investigation and—

(a) search those premises or that information system;

(b) search any person on those premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;

(c) take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation;

(d) demand the production of and inspect relevant licences and registration certificates as provided for in any law;

(e) inspect any facilities on the premises which are linked or associated with the information system and which have a bearing on the investigation;

(f) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to suspect is or has been used in connection with any offence;

(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information system;

(h) require the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system to provide him or her with such reasonable technical and other assistance as he or she may require for the purposes of this Chapter; or

(i) make such inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based, have been complied with.

(2) A person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence.

(3) The Criminal Procedure Act, 1977 (Act No. 51 of 1977), applies with the necessary changes to searches and seizures in terms of this Act.

(4) For purposes of this Act, any reference in the Criminal Procedure Act, 1977, to "premises" and "article" includes an information system as well as data messages.

Obtaining warrant

87. (1) Any court may, upon a request from a cyber inspector but subject to the provisions of section 25 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), issue a warrant required by a cyber inspector in terms of this Chapter.

(2) For the purposes of subsection (1), a court may issue a warrant where—

(a) an offence has been committed within the Republic;

(b) the subject of an investigation is—

(i) a South African citizen or ordinarily resident in the Republic; or

(ii) present in the Republic at the time when the warrant is applied for; or

(c) information pertinent to the investigation is accessible from within the area of jurisdiction of the court.

(3) A warrant to enter, search and seize may be issued at any time and must—

(a) identify the premises or information system that may be entered and searched; and

(b) specify which acts may be performed thereunder by the cyber inspector to whom it is issued.

(4) A warrant to enter and search is valid until—

(a) the warrant has been executed;

(b) the warrant is cancelled by the person who issued it or in that person's absence, by a person with similar authority;

(c) the purpose for issuing it has lapsed; or

(d) the expiry of one month from the date on which it was issued.

(5) A warrant to enter and search premises may be executed only during the day, unless the judge or magistrate who issued it, authorises that it may be executed at any other time.

Preservation of confidentiality

88. (1) Except for the purpose of this Act or for the prosecution of an offence or pursuant to an order of court, a person who has, pursuant to any powers conferred under

this Chapter, obtained access to any information may not disclose such information to any other person.

(2) Any person who contravenes subsection (1) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding six months.

CHAPTER XIII

CYBER CRIME

Definition

89. In this Chapter, unless the context indicates otherwise—

"access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

Unauthorised access to, interception of or interference with data

90. (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so is guilty of an offence.

(2) 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.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program, which is designed primarily to overcome security measures for the protection of data, or performs any of these acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

Computer-related extortion, fraud and forgery

91. (1) A person who performs or threatens to perform any of the acts described in section 90, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence.

(2) A person who performs any of the acts described in section 90 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.

Attempt, and aiding and abetting

92. (1) A person who attempts to commit any of the offences referred to in sections 90 and 91 is guilty of an offence and is liable on conviction to the penalties set out in section 93(1) or (2), as the case may be.

(2) Any person who aids and abets someone to commit any of the offences referred to in sections 90 and 91 is guilty of an offence and is liable on conviction to the penalties set out in section 93(1) or (2), as the case may be.

Penalties

93. (1) A person convicted of an offence referred to in sections 33(2), 41(2), 59(2), 84(5), 86(2) or 90(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.

(2) A person convicted of an offence referred to in section 90(4) or (5) or section 91 is liable to a fine or imprisonment for a period not exceeding five years.

CHAPTER XIV

GENERAL PROVISIONS

Jurisdiction of courts

94. A court in the Republic trying an offence in terms of this Act has jurisdiction where—

(a) the offence was committed in the Republic;

(b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

(c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or

(d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

Saving of common law

95. This Chapter does not affect criminal or civil liability in terms of the common law.

Limitation of liability

96. Neither the State, the Minister, nor any employee of the State is liable in respect of any act or omission in good faith and without gross negligence in performing a function in terms of this Act.

Regulations

97. The Minister may make regulations regarding any matter that may or must be prescribed in terms of this Act or any matter which it is necessary or expedient to prescribe for the proper implementation or administration of this Act.

Short title and commencement

98. This Act is called the Electronic Communications and Transactions Act, 2002, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.

SCHEDULE 1

(see section 4(3))

Item	Column A	Column B
1.	Wills Act, 1953 (Act No. 7 of 1953)	11, 12, 13, 14, 15, 16, 18, 19 and 21
2.	Alienation of Land Act, 1981 (Act No. 68 of 1981)	12 and 13
3.	Bills of Exchange Act, 1964 (Act No. 34 of 1964)	12 and 13
4.	Stamp Duties Act, 1968 (Act No. 77 of 1968)	11, 12, 14

SCHEDULE 2

(see section 4(4))

1.	An agreement for alienation of immovable property as provided for in the Alienation of Land Act, 1981 (Act No. 68 of 1981).
2.	An agreement for the long-term lease of immovable property in excess of 20 years as provided for in the Alienation of Land Act, 1981 (Act No. 68 of 1981).
3.	The execution, retention and presentation of a will or codicil as defined in the Wills Act, 1953 (Act No. 7 of 1953).
4.	The execution of a bill of exchange as defined in the Bills of Exchange Act, 1964 (Act No. 34 of 1964).

MEMORANDUM ON THE OBJECTS OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL, 2002

SUMMARY

The overall objective of the Bill is to enable and facilitate electronic transactions by creating legal certainty around transactions and communications conducted electronically.

The Bill seeks to address the following policy imperatives:

* bridging the digital divide by developing a national e-strategy for South Africa;
* ensuring legal recognition and functional equivalence between electronic and paper-based transactions;
* promoting public confidence and trust in electronic transactions; and
* providing supervision of certain service providers.

Key issues sought to be addressed in the Bill include:

* Maximising benefits — promotion of universal access, especially for members from previously disadvantaged communities, SMMEs and differently abled people;
* Legal certainty — providing for the legally binding effect of electronic transactions and legal recognition of data messages, electronic signatures and electronic evidence;
* E-government — encouraging electronic communication with government;
* Security — the registration of cryptography service providers, the accreditation of electronic signature technologies by authentication service providers, and the protection of critical databases;
* Protection of individuals — protection of the consumer and of privacy as well as of critical data;
* Illegal activities and enforcement — creation of new "cyber offences" and cyber inspectors to administer certain provisions;
* Effective management of Internet-related issues — establishment of a proper management regime with regard to domain names in the Republic and the limitation of liability of Internet service providers.

Chapter I: Interpretation, objects and application

This part of the Bill defines critical words and phrases and sets out the main objects of the Bill.

Chapter II: Maximising benefits and policy framework

The objective is to maximize the benefits the Internet offers by promoting universal and affordable access by all to its possible applications, with a view to bridging the digital divide. The Bill requires the development of a national e-strategy plan by the Minister, in consultation with members of Cabinet. The national e-strategy plan must include detailed plans and programmes to address the development of a national e-transactions strategy, the promotion of universal access and e-readiness, development of SMMEs, empowerment of previously disadvantaged persons and communities, human resource development, and must contain definable objects and timeframes.

Chapter III: Facilitating electronic transactions

This Chapter deals with the removal of legal barriers to electronic transacting. Part 1 provides for the legal recognition of data messages and records. Provision is made for the legal recognition of electronic signatures and "advanced electronic signatures" as a secure form of electronic signing. Electronic data will, subject to certain conditions, be permitted to be retained for statutory record retention purposes, will be regarded as being "in writing", and as a true copy of an "original" record, and provision is made for securing proper evidentiary weight of electronic evidence.

Part 2 deals with the rights and obligations that follow from the communication of data messages, namely contract formation with the time and place of sending and receiving data messages, as well as the time and place where a contract is deemed to

have been formed by means of data messages. The Bill also provides for the validity of sending notices and other expressions of intent through data messages.

Chapter IV: E-government services

This Chapter facilitates electronic filing. It lists the requirements for the production of electronic documents and the integrity of information. Provision is made for a Department or Ministry to accept and transmit documents in the form of electronic data messages, to issue permits or licences in the form of a data message and to make or receive payment in electronic form.

Chapter V: Cryptography providers

The Internet presents security challenges which, without an effective regulatory framework, would pose a threat to the security of consumers and the State. This Chapter requires the suppliers of cryptography materials to register in the prescribed manner their names and addresses, the names of their products and a brief description thereof maintained by the Department of Communications. This will allow investigative authorities such as the SAPS to identify which organisations provide the encryption technologies intercepted by them in terms of our monitoring and interception laws. This will enable the investigative authorities to approach these service providers to assist with deciphering the encrypted messages.

Chapter VI: Authentication service providers

Identification and authentication of the parties in cyberspace remains a challenge and poses threats to consumers and businesses. The Bill seeks to provide for the establishment of an Accreditation Authority within the Department, allowing voluntary accreditation of electronic signature technologies in accordance with minimum standards. Once accredited, these "advanced" electronic signatures will allow a party to rely on their authenticity.

Chapter VII: Consumer protection

Vendors must provide consumers with a minimum set of information, including the price of the product or service, contact details and the right to withdraw from an electronic transaction before its completion. Consumers are also entitled, under certain circumstances, to a "cooling-off" period within which they may cancel certain types of transactions concluded electronically without incurring any penalty. Consumers also have the right not to be bound to unsolicited communications (spam) offering goods or services. The Bill also seeks to place the responsibility on businesses trading on line to make use of sufficiently secure payment systems.

Chapter VIII: Personal information and privacy protection

This Chapter establishes a voluntary regime for protection of personal information. Personal information includes any information that can identify an individual. Collectors of personal information (data collectors) may subscribe to a set of universally accepted data protection principles. It is envisaged that consumers will prefer to deal with only those data collectors that have subscribed to the recorded data protection principles. The sanction for breach of these provisions is left to the parties themselves to agree on. Subscription to these principles is voluntary due to the fact that the South African Law Commission is currently developing specific data protection or privacy legislation which is expected to be enacted within 24 months.

Chapter IX: Protection of critical databases

In terms of its definition, critical data is information which, if compromised, may pose a risk to the national security of the Republic or to the economic or social well-being of its citizens. The Minister may prescribe matters relating to the registration of critical databases and require certain procedures and technological methods to be used in their storage and archiving.

Chapter X: Domain name authority and administration

A section 21 company will be established, or an existing one approved, to manage the domain name space of the Republic. Its membership and governance structures must be representative of the general South African society, Government and other stakeholders. The objects, powers and functions of the Authority are provided for in the Bill. Provision is also made for disputes involving domain names to be settled by means of alternative dispute-resolution methods. The Minister is empowered to formulate national policy on the .za domain name space.

Chapter XI: Limitation of liability of service providers

Chapter XI deals with the limitation of the liability of service providers or so-called "intermediaries" and creates a safe harbour for service providers who are currently exposed to a wide variety of potential liability by virtue of merely fulfilling their basic technical functions. The service providers may seek to limit their liability where they have acted as mere conduits for the transmission of data messages. In each situation the Bill seeks to provide for specific requirements that the actions of the service providers must meet before the clause may be invoked to limit his or her liability.

Chapter XII: Cyber inspectors

Chapter XII of the Bill seeks to provide for the Department of Communications to appoint cyber inspectors. The cyber inspectors may monitor Internet web sites in the public domain and investigate whether cryptography service providers and authentication service providers comply with the relevant provisions. The inspectors are granted powers of search and seizure, subject to obtaining a warrant. Inspectors can also assist the police or other investigative bodies, on request.

Chapter XIII: Cyber crime

Chapter XIII of the Bill seeks to make the first statutory provisions on cyber crime in South African jurisprudence. The Bill seeks to introduce statutory criminal offences relating to information systems and includes—

(a) unauthorised access to data;
(b) interception of or interference with data;
(c) computer-related extortion;
(d) fraud; and
(e) forgery.

Any person aiding or abetting another in the performance of any of these crimes will be guilty as an accessory. The Bill seeks to prescribe the penalties for those convicted of offences.

FINANCIAL IMPLICATIONS FOR STATE

The Bill will lead to new responsibilities for the Department of Communications and to the development of new infrastructure and systems. Consequently, increased financial resources are needed. It will be necessary to equip the required personnel with new skills and proper training, especially technical staff, enabling them to perform the tasks stipulated in the Bill, such as the development and implementation of a national e-strategy plan.

It is anticipated that the Bill will result in changes to certain laws, which may require a review of laws by other Departments. However, the Bill does not oblige government departments to accept or issue documents in electronic form. It merely permits departments to do so. In some instances, such as the establishment of cyber inspectors, the accreditation authority and cryptography, the Department will require re-organisation and restructuring. This will have definite financial implications for the State. However, the Bill will probably effect an increase in the revenue collected by the Department in the form of fees payable for the accreditation of authentication service providers.

OTHER DEPARTMENTS / AGENCIES CONSULTED

The development of the Bill arose out of a lengthy policy-formulation process resulting in a Discussion Paper and Green Paper on Electronic Commerce. This process included extensive consultations with government departments and other stakeholders across the spectrum. Following the conclusion of this consultative process, a legal team comprising of consultants, legal practitioners and academics was appointed. This team, together with officials of the Department, and in consultation with other departments, developed the Bill.

Extensive consultative processes were followed in the development of the Bill:

- An E-Law Conference for all stakeholders was held on 20 and 21 April 2000;
- An Interdepartmental Workshop to discuss the first draft of the Bill was held on 8 May 2001. All Departments were invited and the following Departments and other roleplayers were represented:
  - Department of Justice;
  - South African Law Commission;
  - Departments of Agriculture and of Land Affairs;
  - Department of Foreign Affairs;
  - Government Communication Information System (GCIS);
  - Department of Education;
  - State Information Technology Agency (SITA);
  - Department of Home Affairs;
  - Department of Trade and Industry;
  - Department of Environmental Affairs and Tourism;
  - Department of Public Service and Administration;
  - Department of Health;
  - National Development Agency;
  - Department of Water Affairs and Forestry;
  - Department of Provincial and Local Government;
  - South African Reserve Bank;
  - Department of Labour;
- The draft Bill was sent to all Directors-General of departments for comments;
- Bilateral meetings were held with the following departments to discuss specific issues:
  - Department of Trade and Industry;
  - Department of Labour.

PARLIAMENTARY PROCEDURE

The Department of Communications and the State Law Advisers are of the opinion that the Bill must be dealt with in accordance with the procedure established by section 75 of the Constitution of the Republic since it contains no provision to which the procedure set out in section 74 or 76 of the Constitution applies.