

PARLIAMENT OF THE DEMOCRATIC

SOCIALIST REPUBLIC OF

SRI LANKA

COMPUTER CRIME

ACT, No. 24 OF 2007

[Certified on 09th July, 2007]

Printed on the Order of Government

Published as a Supplement to Part II of the Gazette of the Democratic

Socialist Republic of Sri Lanka of July 13, 2007

PRINTEDAT THE DEPARTMENTOFGOVERNMENT PRINTING, SRILANKA

TO BEPURCHASED AT THEGOVERNMENT PUBLICATIONSBUREAU, COLOMBO 5

Price : Rs. 14.00 Postage : Rs. 7.50

Computer Crime Act, No. 24 of 2007 1

[Certified on 09th July 2007]

L. D.—O. 72/2000

ANACT TO PROVIDE FOR THE IDENTIFICATION OF COMPUTER CRIME AND TO

PROVIDETHE PROCEDURE FOR THEINVESTIGATION AND PREVENTION OF

SUCH CRIMES ; AND TO PROVIDEFOR MATTERS CONNECTED THEREWITH

ANDINCIDENTAL THERETO.

BE it enacted by the Parliament of the Democratic Socialist

Republic of Sri Lanka as follows :-

1. This Act may be cited as the Computer Crime Act, Short title.

No.24 of 2007 and shall come into operation on such date as

the Minister may by Order published in the Gazette appoint

(hereinafter referred to as the “appointed date”).

2. (1) The provisions of this Act shall apply where— Application of

this Act.

(a) a person commits an offence under this Act while

being present in Sri Lanka or outside Sri Lanka ;

(b) the computer, computer system or information

affected or which was to be affected, by the act which

constitutes an offence under this Act, was at the

material time in Sri Lanka or outside Sri Lanka ;

(c) the facility or service, including any computer

storage, or data or information processing service,

used in the commission of an offence under this

Act was at the material time situated in Sri Lanka or

outside Sri Lanka ; or

(d) the loss or damage is caused within or outside Sri

Lanka by the commission of an offence under this

Act, to the State or to a person resident in Sri Lanka

or outside Sri Lanka.

(2) For the purposes of paragraph (d) of subsection (1)

“person” includes a body of persons corporate or

unincorporate.

2 Computer Crime Act, No. 24 of 2007

PART I

COMPUTER CRIME

Securing 3. Any person who intentionally does any act, in order

unauthorised to secure for himself or for any other person, access to—

access to a

computer an

offence. (a) any computer ; or

(b) any information held in any computer,

knowing or having reason to believe that he has no lawful

authority to secure such access, shall be guilty of an offence

and shall on conviction be liable to a fine not exceeding one

hundred thousand rupees, or to imprisonment of either

description for a term which may extend to five years, or both

such fine and imprisonment.

Doing any act to 4. Any person who intentionally does any act, in order

secure to secure for himself or for any other person, access to—

unauthorised

access in order to

commit an (a) any computer ; or

offence

(b) any information held in any computer,

knowing or having reason to believe that he has no lawful

authority to secure such access and with the intention of

committing an offence under this Act or any other law for the

time being in force, shall be guilty of an offence and shall on

conviction be liable to a fine not exceeding two hundred

thousand rupees or to imprisonment of either description for

a term which may extend to five years or to both such fine

and imprisonment.

Explanation 1— for the purposes of paragraph (a)

the mere turning on of a computer is sufficient.

Explanation 2— for the purposes of paragraph (b)-

(a) there should be an intention to sccure any programme or

data held in any computer ;

Computer Crime Act, No. 24 of 2007 3

(b) the access intended to be sccured, should be unauthorised;

(c) it is not necessary to have access directed at any particular

programme, data or computer.

5. Any person who, intentionally and without lawful Causing a

computer to

authority causes a computer to perform any function knowing perform a

or having reason to believe that such function will result in function without

unauthorised modification or damage or potential damage lawful authority

an offence.

to any computer or computer system or computer programme

shall be guilty of an offence and shall on conviction be liable

to a fine not exceeding three hundred thousand rupees or to

imprisonment of either description for as term which may

extend to five years or to both such fine and imprisonment.

Illustrations

For any unauthorised modification or damage or potential

damage to any computer or computer system or computer

programme to take place, any one of the following may occur:—

(a) impairing the operation of any computer, computer

system or the reliability of any data or information

held in any computer; or

(b) destroying, deleting or corrupting, or adding, moving

or altering any information held in any computer;

(c) makes use of a computer service involving computer

time and data processing for the storage or retrieval

of data;

(d) introduces a computer program which will have the

effect of malfunctioning of a computer or falsifies

the data or any information held in any computer or

computer system.

4 Computer Crime Act, No. 24 of 2007

Explanation- for the purposes of paragraphs (a) to

(d) above, it is immaterial whether the consequences

referred to therein were of a temporary or permanent

nature.

Offences 6. (1) Any person who intentionally causes a computer

committed to perform any function, knowing or having reason to believe

against national

that such function will result in danger or imminent danger

security &c.

to—

(a) national security ;

(b) the national economy ; or

(c) public order,

shall be guilty of an offence and shall on conviction be

punishable with imprisonment of either description for a term

not exceeding five years.

(2) In a prosecution for an offence under paragraphs (a) or

(c) of subsection (1), a Certificate under the hand of the

Secretary to the Ministry of the Minister in charge of the

subject of Defence or, in a prosecution for an offence under

paragraph (b) of subsection (1), a Certificate under the hand

of the Secretary to the Ministry of the Minister in charge of

the subject of Finance, stating respectively, that the situation

envisaged in subsection (1) did in fact exist in relation to

national security or public order, or the national economy, as

the case may be, shall be admissible in evidence and shall be

prima facie evidence of the facts stated therein.

Dealing with 7. Any person who, knowing or having reason to believe

data &c., that any other person has without lawful authority obtained

unlawfully

information from a computer or a storage medium of a

obtained an

offence. computer,—

(a) buys, receives, retains, sells, or in any manner deals

with ; or

Computer Crime Act, No. 24 of 2007 5

(b) offers to buy or sell, or in any manner deals with ; or

(c) downloads, uploads, copies or acquires the

substance or meaning of,

any such information shall be guilty of an offence and shall

on conviction be liable to a fine not less than one hundred

thousand rupees and not exceeding three hundred thousand

rupees or to imprisonment of either description for a term not

less than six months and not exceeding three years, or to

both such fine and imprisonment.

Explanation .—For the purposes of sections 9 and 10—

(a) It is immaterial that the offender had

authority to access the computer or had

authority to perform the function ;

(b) The offender need not have intended

to cause or have had the knowledge

that he is likely to cause, loss or damage

to any particular person or institution.

8. Any person, who, knowingly or without lawful Illegal

authority intercepts— interception of

data an offence.

(a) any subscriber information or traffic data or any

communication, to, from or within a computer ; or

(b) any electromagnetic emissions from a computer that

carries any information,

shall be guilty of an offence and shall on conviction be liable

to a fine not less than one hundred thousand rupees and not

exceeding three hundred thousand rupees or to imprisonment

of either description for a term not less than six months and

not exceeding three years, or to both such fine and

imprisonment.

6 Computer Crime Act, No. 24 of 2007

Using of illegal 9. Any person who, without lawful authority produces,

devices an sells, procures for use, imports, exports, distributes or otherwise

offence.

makes available—

(a) any device, including a computer or computer

program ;

(b) a computer password, access code or similar

information by which the whole or any part of a

computer is capable of being accessed,

with the intent that it be used by any person for the purpose

of committing an offence under this Act shall be guilty of an

offence and shall on conviction be liable to a fine not less

than one hundred thousand rupees and not exceeding

three hundred thousand rupees or to imprisonment of

either description for a term not less than six months and

not exceeding three years, or to both such fine and

imprisonment.

Unauthorised 10. Any person who, being entrusted with information

disclosure of which enables him to access any service provided by means

information

of a computer, discloses such information without any express

enabling access

to a service, an authority to do so or in breach of any contract expressed or

offence. implied, shall be guilty of an offence and shall on conviction

be liable to a fine not less than one hundred thousand rupees

and not exceeding three hundred thousand rupees or to

imprisonment of either description for a term not less than

six months and not exceeding three years or to both such fine

and imprisonment.

Attempts to 11. Any person who attempts to commit an offence under

commit offence. sections 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 of this Act or

to cause such an offence to be committed, shall be guilty of

an offence and shall on conviction be liable to a fine not

exceeding one half of the maximum fine provided for each of

such offences, or to imprisonment of either description for a

term not exceeding one half of the maximum term provided

for each of such offences, or to both such fine and

imprisonment.

Computer Crime Act, No. 24 of 2007 7

12. (1) Any person who abets the commission of an Abetment of an

offence under this Act shall be guilty of the offence of offence.

abetment and shall on conviction—

(a) if the offence abetted is committed in consequence

of the abetment, be liable to the same punishment

as is provided for the offence; and

(b) if the offence is not committed in consequence of

the abetment, be liable —

(i) where the maximum fine or term of

imprisonment is provided for, to a fine not

exceeding one fourth of the maximum fine

provided for the offence or to imprisonment

of either description for a term not exceeding

one fourth of the maximum term provided for

the offence, or to both such fine and

imprisonment; and

(ii) where the maximum fine or imprisonment is

not provided for or the maximum term of

imprisonment is life, to a fine not exceeding

two hundred and fifty thousand rupees or to

imprisonment of either description for a term

not exceeding five years, or to both such fine

and imprisonment.

(2) The term ‘abet’ shall have the same meaning as in

sections 100 and 101 of the Penal Code (Chapter 19) and the

provisions of sections 101A, 103, 104, 105, 106 and 107 of

the Penal Code (Chapter 19) shall mutatis mutandis apply in

relation to the abetment of any offence under this Act.

13. (1) Any person who conspires to commit an offence Conspiring to

under this Act shall be guilty of an offence and shall, on commit an

offence.

conviction be liable to be punished with the punishment

prescribed for abetting the commission of that offence.

8 Computer Crime Act, No. 24 of 2007

(2) The term “conspire” shall have the same meaning as

in subsection (2) of section 113A of the Penal Code (Chapter

19) and the provisions of that section shall mutatis mutandis

apply in relation to conspiracy to commit any offence under

this Act.

Compensation to

be awarded for 14. (1) Where a person is convicted of an offence under

loss or damage this Act, and where it is established that as a result of the

consequent to an commission of such offence—

offence.

(a) loss or damage was caused to any person or

institution; or

(b) monetary gain accrued to the offender or any other

person,

the court shall, in addition to any other punishment that may

be imposed on the offender, make order for the payment by

the offender—

(i) of compensation, to the person or institution that

incurred loss or damage; or

(ii) of a sum equivalent to the value of the monetary

gain so accrued, to the State, as the case may be.

(2) An order made under subsection (1) for payment, shall

be enforced as if such order was a decree entered by the District

Court in favour of the person or institution which suffered

the loss or damage or the State, as the case may be.

(3) A Certificate under the hand of an expert containing a

record of the quantum of compensation as computed by the

victim and a statement whether in the opinion of the expert,

the quantum of compensation is proportionate to the loss or

damage caused or the monetary value of the gain accrued

shall be admissible in evidence and shall be prime facie proof

of the facts stated therein.

Computer Crime Act, No. 24 of 2007 9

(4) An order under subsection (1) for the payment of

compensation in favour of any person shall not debar or

prejudice any right of that person to a civil remedy for the

recovery of damages :

Provided however that the time limit specified in the

Prescription Ordinance (Chapter 68) for the commencement

of any action relating to a civil remedy, shall, for the purposes

of this Act, be computed only from the date on which an

order under subsection (1) is made.

PART II

INVESTIGATIONS

15. Except as otherwise provided by this Act, all offences Offences under

under this Act shall be investigated, tried or otherwise dealt this Act to be

investigated

with in accordance with the provisions of the Code of Criminal under the

Procedure Act, No. 15 of 1979. provisions of the

Code of Criminal

Procedure.

16. Every offence under this Act shall be a cognizable Offence under

offence within the meaning of, and for the purpose of, the the Act to be

cognizable

Code of Criminal Procedure Act, No. 15 of 1979.

offence.

17. (1) The Minister in charge of the subject of Science Appointment of

and Technology may, in consultation with the Minister in a panel of

experts.

charge of the subject of Justice, appoint by Order puiblished

in the Gazette any public officer having the required

qualification and experience in electronic engineering or

software technology (hereinafter referred to as“an expert”) to

assist any police officer in the investigation of an offence

under this Act.

(2) For the purposes of this section “expert” includes-

(a) any member of the staff of any University who

possesses the prescribed qualification and, who is

nominated by the Vice-Chancellor of the relevant

University ;

10 Computer Crime Act, No. 24 of 2007

(b) any public institution which in the opinion of

the relevant University possesses the prescribed

qualification and is nominated by the

Vice-Chancellor of such University :

Provided that where an “expert” cannot be

identified in terms of paragraph (a) or (b) above the

Minister may, in consultation with the Vice-

Chancellor of the relevant University appoint any

other institution which satisfies the prescribed

qualification ;

(c) University shall mean any University established

under the Universities Act, No. 16 of 1978.

(3) The qualifications and experience (having regard to

the specific areas of expertise in electronic engineering or

software technology) required to be fulfilled by an officer

appointed under subsection (1) and the manner and mode of

appointment and the conditions of appointment of such

officer shall be as prescribed by regulations.

(4) For the purpose of an investigation under this Act, an

expert called upon to assist any police officer shall, have the

power to—

(a) enter upon any premises along with a police officer

not below the rank of a sub-inspector ;

(b) access any information system, computer or

computer system or any programme, data or

information held in such computer to perform any

function or to do any such other thing ;

(c) require any person to disclose any traffic data ;

(d) orally examine any person ;

(e) do such other things as may be reasonably required,

for the purposes of this Act.

Computer Crime Act, No. 24 of 2007 11

(5) An expert shall be paid such remuneration as may be

determined by the Minister in consultation with the Minister

in charge of the subject of Finance.

(6) An expert may be called upon to assist any police

officer in the investigation of an offence under this Act and it

shall be duty of the officer to render all such assistance as

may be required for the purposes of such investigation. Where

any proceedings have been commenced consequent to the

findings of an investigation, it shall be the duty of the officer

to make available for the purposes of such proceedings, any

information, data, material or other matter that may be

obtained by him in the course of such investigation.

18. (1) An expert or a police officer may, for the purposes Powers of search

of an investigation under this Act under the authority of a and seizure with

warrant.

warrant issued in that behalf by a Magistrate on application

made for such purpose,—

(i) obtain any information including subscriber

information and traffic data in the possession of any

service provider;

(ii) intercept any wire or electronic communication

including subscriber information and traffic data, at

any stage of such communication.

(2) Notwithstanding the provisions of subsection (1), an

expert or a police officer may without a warrant exercise all

or any of the powers referred to in that subsection, if—

(a) the investigation needs to be conducted urgently;

and

(b) there is a likelihood of the evidence being lost,

destroyed, modified or rendered inaccessible; and

(c) there is a need to maintain confidentiality regarding

the investigation.

12 Computer Crime Act, No. 24 of 2007

(3) The provisions of sections 36, 37 and 38 of the Code of

Criminal Procedure Act, No. 15 of 1979 shall not apply in

relation to the arrest of a person for an offence under this Act.

(4) The Minister may by regulation prescribe the manner

in which and the procedures required to be followed in respect

of, the retention and interception of data and information

including traffic data, for the purposes of any investigation

under this Act.

Preservation of 19. (1) Where an expert or a police officer is satisfied

information. that any information stored in a computer is reasonably

required for the purposes of an investigation under this Act

and that there is a risk that such information may be lost,

destroyed, modified or rendered inaccessible, he may by

written notice require the person in control of such computer

or computer system to ensure that the information be preserved

for such period not exceeding seven (07) days as may be

specified in such notice.

(2) On an application made to a Magistrate having

jurisdiction, the period for which the information is to be

preserved may be extended for such further period, which in

the aggregate shall not exceed upto ninety days.

Normal use of 20. Every police officer and every expert who conducts

computer not to any search, inspection or does any other thing in the course

be hampered.

of an investigation, shall make every endeavour to ensure

that the ordinary course of legitimate business for which any

computer may be used is not hampered by such search,

inspection or investigation and shall not seize any computer,

computer system or part thereof, if such seizure will prejudice

the conduct of the ordinary course of business for which the

computer is used, unless—

(a) it is not possible to conduct the inspection on the

premises where such computer, computer system or

part thereof is located; or

Computer Crime Act, No. 24 of 2007 13

(b) seizure of such computer, computer system or part

thereof is essential to prevent the commission of the

offence or the continuance of the offence or to obtain

custody of any information which would otherwise

be lost, destroyed, modified or rendered inaccessible.

21. (1) Any police officer may, in the course of an Power of police

investigation under this Act, exercise powers of arrest, search, officer to arrest,

search and seize.

or seizure of any information accessible within any premises,

in the manner provided for by law:

Provided that a police officer making an arrest without a

warrant of person suspected of committing an offence under

this Act, shall without unnecessary delay and within twenty-

four hours of such arrest, exclusive of the time taken for the

journey from the place of arrest to the presence of the

Magistrate, produce such person before the Magistrate of the

Court nearest to the place that the suspect is arrested.

(2) No police officer shall access any computer for the

purpose of an investigation under this Act unless the Inspector

General of Police has certified in writing that such police

officer possesses adequate knowledge and skill in the field

of information communication technology and is thereby

possessed of the required expertise to perform such a function.

22. (1) Where any item or data has been seized or Police officer to

rendered inaccessible in the course of an investigation, the record and

afford access to

police officer conducting the search shall issue a complete

seized data.

list of such items and data including the date and time of

such seizure or of rendering it inaccessible to the owner or

person in charge of the computer or computer system.

(2) Subject to the provisions of subsection (3), a police

officer may upon application made by the owner or person in

control of the computer or computer system, permit a person

nominated by such owner or person to issue such person a

copy of such data.

14 Computer Crime Act, No. 24 of 2007

(3) A police officer shall not grant permission or give such

copies under subsection (2) if it appears that such permission

would be prejudicial to any criminal investigation or

proceeding.

Duty to assist 23. (1) Any person who is required to make any disclosure

investigation. or to assist in an investigation under this Act, shall comply

with such requirement.

(2) A person who obstructs the lawful exercise of the powers

conferred on an expert or a police officer or fails to comply

with such request made by such expert or police officer during

an investigation shall be guilty of an offence and shall on

conviction be liable to a fine not exceeding two hundred

thousand rupees or to imprisonment of either description for

a period not less than one year and not exceeding two years

or to both such fine and imprisonment.

Confidentiality 24. (1) Every person engaged in an investigation under

of information this Act shall maintain strict confidentiality with regard to

obtained in the

course of an all information as may come to his knowledge in the course

investigation. of such investigations and he shall not disclose to any person

or utilize for any purpose whatsoever any information so

obtained other than in the discharge of his duties under this

Act.

(2) Every service provider from whom any information

has been requested or obtained and any person to whom a

written notice has been issued for the preservation of any

information shall maintain strict confidentiality in relation

to such information and the fact that such information has

been requested, obtained or required to be preserved, and

shall not make any disclosure in regard to such matters other

than with lawful authority.

(3) A service provider shall not be held liable under the

civil or criminal law for the disclosure of any data or other

information for the purposes of an investigation under this

Act.

Computer Crime Act, No. 24 of 2007 15

(4) Any person who contravenes the provisions of

subsections (1) and (2) shall commit an offence and shall on

conviction be liable to a fine not exceeding three hundred

thousand rupees or to imprisonment of either description for

a term not exceeding two years or to both such fine and

imprisonment.

PART III

MISCELLANEOUS

25. The jurisdiction to hear, try and determine all Jurisdiction.

offences under this Act shall be vested with the High Court :

Provided however that where the provisions of the

Extradition Law, No. 8 of 1977 is applicable in relation to

the commission of an offence under this Act, the High Court

holden at Colombo shall have exclusive jurisdiction to hear,

try and determine such offence.

26. (1) Every document duly signed and issued by an Proof of

expert or a police officer, as the case may be, and duly document issued

by an expert or a

authenticated by an expert in the prescribed manner, shall be

Police Officer.

admissible in evidence and shall be prima facie evidence of

the facts stated therein.

(2) for the purposes, of this section the expression

“document” shall include a certificate, declaration,

information, data, report or any other similar document.

27. The Schedule to the Extradition Law, No. 8 of 1977 Amendment of

is hereby amended by the insertion immediately before Part the Schedule to

the Extradition

B thereof, of the following new item :—

Law, No. 8 of

1977.

“(49) An offence committed in terms of the Computer

Crimes Act, No. 24 of 2007.”.

28. No civil or criminal action shall be instituted against Immunity from

an expert or a police officer appointed for the purpose of this legal

proceedings.

Act, for any lawful act which is done or purported to be done

in good faith by such expert or police officer as the case may

be, in pursuance of his duties under this Act.

16 Computer Crime Act, No. 24 of 2007

Experts deemed 29. Every expert shall, in the discharge of his duties

to be peace under this Act, be deemed to be—

officer and

public officer.

(a) a “peace officer” within the meaning and for the

purposes of the Code of Criminal Procedure Act,

No. 15 of 1979; and

(b) a “public officer” within the meaning and for the

purposes of the Penal Code (Chapter 19).

Offences by 30. Where an offence under this Act is committed by a

bodies of body of persons, then if that body of person is—

persons.

(a) a body corporate, every director and officer of that

body corporate; or

(b) a firm, every partner of that firm; or

(c) a body unincorporated other than a firm, every

officer of that body responsible for its management

and control,

shall be deemed to be guilty of such offence :

Provided that no such person shall be deemed to be guilty

of such offence if he proves that such offence was committed

without his knowledge or that he exercised all due diligence

to prevent the commission of such offence.

Presumptions. 31. For the purposes of the application of the provisions

of the Penal Code (Chapter 19) in relation to an offence

committed under this Act—

(a) an offence under this Act committed outside the

territory of Sri Lanka shall be deemed to have been

committed in Sri Lanka; and

(b) any information referred to in this Act shall be

deemed to be property.

Computer Crime Act, No. 24 of 2007 17

32. (1) The Minister may make regulations under this Regulations.

Act for the any matter authorized or required to be made

under this Act, or which in required to be prescribed under

this Act, or for the purpose of carrying out or giving effect to

the principles and provisions of this Act.

(2) Every regulation made by the Minister shall be

published in the Gazette and shall come into operation on

the date of such publication or on such later date as may be

specified in the regulation.

(3) Every regulation made by the Minister shall as soon

as convenient after its publication in the Gazette be brought

before Parliament for its approval. Any regulation which is

not so approved shall be deemed to be rescinded as from the

date of disapproval but without prejudice to anything

previously done thereunder.

(4) Notification of the date on which a regulation is

deemed to be rescinded shall be published in the Gazette.

33. Where a request is made to the Government of Sri Minister to

Lanka, by or on behalf of another Government for the notify requesting

State, of

extradition of any person accused or convicted of an offence

measures taken

under this Act, the Minister shall on behalf of the Government against persons

of Sri Lanka, forthwith notify the Government of the for whose

requesting State of the measures which the Government of extradition

request is made.

Sri Lanka has taken, or proposes to take, for the prosecution

or extradition of that person for that offence.

34. Where a person who is not a citizen of Sri Lanka is Rights of certain

arrested for an offence under this Act, such person shall be persons arrested

for offences

entitled— under this Act.

(a) to communicate without delay, with the nearest

appropriate representative of the State of which he

is a national or which is otherwise entitled to protect

his rights or if he is a stateless person, with the nearest

appropriate representative of the State in the territory

of which he was habitually resident ; and

18 Computer Crime Act, No. 24 of 2007

(b) to be visited by a representative of that State; and

(c) be informed of his rights under paragraphs

(a) and(b).

Assistance to 35. (1) The provisions of the Mutual Assistance in

Convention Criminal Matters Act, No. 25 of 2002 shall, wherever it is

States &c.

necessary for the investigation and prosecution of an offence

under this Act, be applicable in respect of the providing of

assistance as between the Government of Sri Lanka and other

States who are either Commonwealth countries specified

by the Minister by Order under section 2 of the aforesaid

Act or Non-Commonwealth countries with which the

Government of Sri Lanka entered into an agreement in terms

of the aforesaid Act.

(2) In the case of a country which is neither a

Commonwealth country specified by the Minister by Order

under section 2 of the aforesaid Act nor a Non-Commonwealth

country with which the Government of Sri Lanka entered

into an agreement in terms of the aforesaid Act, then it shall

be the duty of the Government to afford all such assistance

to, and may through the Minister request all such assistance

from, a convention country, as may be necessary for the

investigation and prosecution of an offence under this Act

(including assistance relating to the taking of evidence and

statements, the serving of process and the conduct of searches).

(3) The grant of assistance in terms of this section may be

made subject to such terms and conditions as the Minister

thinks fit.

Offences under 36. Notwithstanding anything in the Extradition Law,

this Act, not to No. 8 of 1977, an offence specified in the Schedule to that

be political

Law and in this Act, shall for the purposes of that law be

offences &c., for

the purposes of deemed not to be an offence of a political character or an

the Extradition offence connected with a political offence or an offence

Law. inspired by political motives, for the purposes only of the

extradition of any person accused or convicted of any such

offence, as between the Government of Sri Lanka and any

requesting State, or of affording assistance to a requesting

State under section 35.

Computer Crime Act, No. 24 of 2007 19

37. In the event of any inconsistency between the Sinhala Sinhala text to

and Tamil texts of this Act, the Sinhala text shall prevail. prevail in the

event of

inconsistency.

38. In this Act, unless the context otherwise requires,— Interpretation.

“computer” means an electronic or similar device having

information processing capabilities;

“storage medium” means any [electronic or similar device]

from which information is capable of being

reproduced, with or without the aid of any other

article or device;

“computer programme” means a set of instructions

expressed in words, codes, schemes or any other

form, which is capable when incorporated in a

medium that the computer can read, of causing a

computer to perform or achieve a particular task ;

“computer system” means a computer or group of inter-

connected computers, including the internet;

“document” includes an electronic record;

“electronic record” means, information, record or data

generated, stored, received or sent in an electronic

form or microfilm, or by any other similar means;

“function” in relation to a computer, includes logic, control

or carrying out of an arithmetical process, deletion,

storage and retrieval and communication to or within

a computer;

“information” includes data, text, images, sound, codes,

computer programmes, databases or microfilm;

“service provider” means—

(a) a public or private entity which provides the

ability for its customers to communicate by

means of a computer system; and

20 Computer Crime Act, No. 24 of 2007

(b) any other entity that processes or stores

computer data or information on behalf of that

entity or its customers;

“subscriber information” means any information,

contained in the form of computer data or any other

form that is held by a service provider, relating to

subscribers of its services;

“traffic data” means data—

(a) that relates to the attributes of a

communication by means of a computer

system;

(b) data generated by a computer system that is

part of a service provider; and

(c) which shows communications origin,

destination, route, time, data, size, duration

or details of subscriber information.

Annual subscription of English Bills and Acts of the Parliament Rs. 885 (Local), Rs. 1,180

(Foreign), Payable to the SUPERINTENDENT, GOVERNMENT PUBLICATIONS BUREAU, DEPARTMENT OF

GOVERNMENT INFORMATION, NO. 163, KIRULAPONA AVENUE, POLHENGODA, COLOMBO 05 before

15th December each year in respect of the year following.