

INDEX

CHAPTER 1 The general nature of crimes

1.1	Introduction	1
1.2	General nature of crimes	2
1.3	Criminal Law	4
1.4	What is a crime?	5
1.5	Main elements of a crime	5
1.6	Doctrine of Mens Rea	6
1.7	Doctrine of Mens Rea under the Sri Lankan law	10
1.8	Individual and corporate liability in criminal cases	12
1.9	Defences available in a criminal case	14
1.10	Proof of a crime	16
1.11	Proof of a defence	16

CHAPTER 2 The nature of computer crime

2.1	What is a crime? The traditional approach in the United Kingdom	21
2.2	The development of the English Criminal Law	22
2.3	The hearing of criminal offences	24
2.4	Information Technology and crime	25
2.5	What are the crimes that could be committed through the use of a computer?	27
2.6	Element of deception	28
2.7	Element of "property belonging to another"	30

CHAPTER 3 Computer crimes of a traditional nature

3.1	Traditional crimes- the Law in the United Kingdom	35
3.2	Input fraud	36
3.3	Output fraud	37
3.4	Data fraud	38
3.5	Program fraud	38
3.6	Traditional crimes	38
3.6.1	Obtaining property by deception	38
3.6.2	Obtaining a money transfer by deception	37
3.6.3	Conspiracy to defraud	39
3.6.4	Theft	40
3.6.5	Attempts	42

CHAPTER 4 Offences under the Companies Misuse Act of 1990 of the United Kingdom

4.1	Introduction	45
4.2	Unauthorized access to computer material	47
4.3	Unauthorized access with intent to commit or facilitate commission of other offences (Ulterior intent offence)	55
4.4	Unauthorized modification of computer material	58
4.5	Unauthorized modification of computer material by a person who has authority to gain access	60

CHAPTER 5 Computer Crimes - The Sri Lankan experience- Issues prior to the enactment of the law

5.1	Introduction	65
5.2	The existing law (prior to the enactment of the Computer Crimes Act)	67

5.3	The initiative for law reform	76
CHAPTER 6 The applicability and the main provisions of the Computer Crimes Act No. 24 of 2007		81
CHAPTER 7 Identified offences under the Computer Crimes Act- Offences relating to unauthorized access		
7.1	Introduction	87
7.2	Scope of section 3	88
7.3	Defences	94
7.4	Some specific issues	95
CHAPTER 8 Ulterior intent offence		
8.1	Introduction	99
8.2	Defences	102
8.3	Some specific issues	102
CHAPTER 9 Unauthorized modification of material		
9.1	Introduction	108
9.2	Defences	109
9.3	Computer viruses	110
CHAPTER 10 Offences against National Security, Public Security and National Economy		
10.1	Introduction	115
10.2	Defences	117
CHAPTER 11 Involvement with data illegally obtained		
11.1	Introduction	119
11.2	Defences	123

11.3	Some specific issues	124
CHAPTER 12 Illegal interception of data		
12.1	Introduction	127
12.2	Defences	128
CHAPTER 13 Using of illegal devices		
13.1	Introduction	131
13.2	Defences	132
CHAPTER 14 Unauthorized disclosure of information enabling access to a service		
14.1	Introduction	135
14.2	Defences	136
CHAPTER 15 Attempts to commit offences and abetment and conspiracy		
15.1	Attempts	139
15.2	Abetment	139
15.3	Conspiracy	141
CHAPTER 16 Awarding of compensation		
16.1	Introduction	146
CHAPTER 17 Investigation of offences under the Act		
17.1	Introduction	153
17.1.1	Procedure	153
17.1.2	Nature of offences	153
17.2	Appointment of experts	154
17.3	Powers of the experts	154

CHAPTER 18 Powers of search and seizure

18.1	Introduction	157
18.2	Protection of data	159
18.3	Duty on police officers and experts	160
18.4	Arrest, search and seizure of information	162
18.5	Duty of police officers upon seizure	163
18.6	Secrecy	164

CHAPTER 19 Miscellaneous Provisions

19.1	Jurisdiction	169
19.2	Admissibility of evidence	170
19.3	Application of the extradition law	170
19.4	Immunity from legal proceedings	171
19.5	Experts to be considered as peace officers and public officers	171
19.6	Corporate criminal liability	172
19.7	Presumptions	173
19.8	Regulations by the Minister	174
19.9	Role of the State in case of an application for extradition	175
19.10	Rights of certain persons	175
19.11	Assistance for convention States	176
19.12	Application of the extradition law	177
19.13	Definitions	178

CHAPTER 20 Related issues and the position in English Law

20.1	Communication offences	183
20.2	Blackmail	184
20.3	Pornography	185
20.4	The law relating to phonographic messages under the law of Sri Lanka	186
20.5	Intellectual Property offences	189
20.5.1	History	189

20.5.2	Patents	192
20.5.3	Trade Marks	192
20.5.4	Trade Names	195
20.5.5	Industrial designs	196
20.5.6	Copyright	198

CHAPTER 21 Computer Evidence

21.1	Law of Evidence in Sri Lanka	203
21.2	Evidence (Special Provisions) Act No 14 of 1995	205
21.3	Computer Evidence under Act No. 14 of 1995	208

CHAPTER 22 Some relevant issues

22.1	Employment contracts	215
22.2	Security measures	215
22.3	What is cyber security?	215
22.4	What are the risks?	216
22.5	What can you do?	216
22.6	Guidelines to be followed in publishing information online	218
22.7	Why is it important to remember that the internet is public?	218
22.8	What guidelines can you follow when publishing information on the internet?	219
22.9	Good security habits	220
22.10	How can you minimize the access other people have to your information?	221
22.11	What other steps can you take?	222
22.12	Safeguarding your data	223
22.13	How can you protect both your personal and work-related data?	224

CHAPTER 23	Relevant case law	229
	Reading Material on Computer Crimes law	249
	The Computer Crimes Act	251