RAND EUROPE

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Europe

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.

This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL REPORT

Handbook of Legal Procedures of Computer and Network Misuse in EU Countries

Lorenzo Valeri, Geert Somers, Neil Robinson,
Hans Graux, Jos Dumortier

Prepared for the European Commission

RAND EUROPE

lawfort

The research described in this report was prepared for the European Commission.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2006 the European Commission

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the copyright holder.

Published 2006 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
Newtonweg 1, 2333 CP Leiden, The Netherlands
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
Uhlandstraße 14, 10623 Berlin, Germany
RAND URL: http://www.rand.org/
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

In 2003 the European Commission commissioned RAND Europe to develop a Handbook that provided an easy to use guide matching technical descriptions of incidents to the legal framework of the country in question, and detailed procedures for working with law enforcement to respond to incidents. This handbook was tailored to the user requirements of Europe's Computer Security Incident Response Team (CSIRT) community. RAND Europe and Lawfort were invited to update this first version of the Handbook, to take into account the recent developments in the legal framework in the EU and more importantly, to extend its scope to cover the situation in the 10 new Member States which joined the European Union on 1st May 2004. The MODINIS work programme supports this activity under the heading of "favouring co-ordination between CSIRTs." This project is also undertaken as a preparatory activity for the newly formed European Network and Information Security Agency (ENISA).

This is the final report of the 2005 EC-CSIRT Legal Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for Assisting Computer Security Incident Response Teams (CSIRTS): hereafter '2005 CSIRT Legal Handbook'.

In detail, the CSIRT Legal Handbook provides user-friendly access to up to date information on rules and regulations concerning computer misuse and the collection and reporting of computer evidence currently in force in all 25 EU countries, together with guidelines as to when and how law enforcement must be informed of incidents. The project will update the taxonomy, review and analyse standard enquires and reporting needs, survey national legal frameworks and relevant industrial initiatives and provide a user friendly electronic application for modifying and updating the information.

Project co-ordination and management, the user survey and design and implementation of the electronic applicaition was conducted by RAND Europe, an independent not-for-profit policy research organisation that serves the public interest by improving policymaking and informing public debate. Lawfort, a leading and independent Belgian law firm (www.lawfort.be) with offices Brussels, Antwerp, Ghent and Liège, conducted and managed the contributions of national legal correspondents across the EU under the leadership of Professor Jos Dumortier. These are detailed in the table below:

Member State	Principal source(s)
Austria	Dr. Erich Schweighofer and Dr. Doris Liebwald, Wiener Zentrum für Rechtsinformatik, Universität Wien
Belgium	Prof Jos Dumortier, Geert Somers, Hans Graux, Lawfort
Cyprus	Olga Georgiades, Lawyer, Lellos P Demetriades Law Office
Czech	Jan Hobza, Sales Manager Siemens Business Services Ltd, and Kubo Macak, LL.M.
Danmark	Dr. Henrik Udsen, University of Copenhagen
Estonia	Tõnu Lausmaa, Re-En Center TAASEN
Finland	Kirsi Kankare, LL.M., Sourcing Manager Nokia
Germany	Marian Alexander Arning, LL.M. and Dr. Kai Cornelius, LL.M.
Greece	Konstantinos Kyrmanidis, Lawyer
Hungary	Dr. Koppányi Szabolcs, LL.M.
Italy	Paolo Galdieri, Lawyer
Latvia	Andris Kikans and Juris Breicis, Datorzinibu Centrs A/S
Lithuania	Mindaugas Civilka, Lawyer, Law Offices Norcous & Partners
Malta	Dr. Olga Finkel, Lawyer, Gatt Frendo Tufigno Advocates
Poland	Hon. Dariusz Sielicki, judge, legal expert for the Polish Ministry of Justice
Portugal	Pedro Simões Dias, Lawyer, Uría & Menéndez Lisboa
Slovakia	JUDr. Martin Lupták, Public Prosecutor and External Professor Univerzity Mateja Bela
Slovenia	Gorazd Božič, ARNES SI-CERT
Spain	Joaquín de Otaola, Lawyer, Sanchez Pintado, Núñez & Asociados, S.L.
Sweden	Patrik Håkansson, DCI / IT Crime Squad, National Criminal Police Sweden
United Kingdom	Peter Sommer, London School of Economics

For more information this project please contact Dr Lorenzo Valeri, at the Information Society Programme, (lvaleri@rand.org) at the following address:

Dr Lorenzo Valeri
Information Society Programme
RAND Europe
Westbrook Centre
Milton Road
Cambridge
CB4 1YG
UNITED KINGDOM
lvaleri@rand.org
T: +44(0)1223 353329

Contents

Preface ii

Executive Summary **10**

Country Reports **12**

CHAPTER 1 **Introduction to Country Reports** **13**
1.1 Taxonomy of Information Security Incidents 13
1.2 The Criminality of Incidents across the EU 15
1.3 Matching incidents to the Framework Decision and Council of Europe Cyber-Crime Convention 18

CHAPTER 2 **Country Report - Austria** **24**
2.1 Austrian Legislation on Computer Crimes 24
2.2 Law Enforcement Bodies 28
2.2.1 Police (www.polizei.gv.at) 28
2.2.2 Austrian Administrative Adjudication 29
2.2.3 Austrian Criminal Proceedings 29
2.3 Reporting 30
2.3.1 Competent Authorities 30
2.3.2 Contact Details 30
2.4 Forensics 31
2.5 References 32

CHAPTER 3 **Country Report: Belgium** **34**
3.1 Belgian legislation on computer crimes 34
3.2 Law enforcement bodies 36
3.2.1 Police (www.police.be) 36
3.2.2 Courts (www.cass.be) 37
3.3 Reporting 37
3.3.1 Competent authorities 37
3.3.2 Contact details 37
3.3.3 Other reporting mechanisms 37
3.4 Forensics 38
3.4.1 Data seizure 39

3.4.2 Network searching 39
3.4.3 Involvement of experts 39
3.5 References (www.just.fgov.be) 40

CHAPTER 4 **Country report - Cyprus 41**
4.1 Cypriot legislation on computer crimes 41
4.2 Law enforcement bodies 50
4.2.1 Police (www.police.gov.cy) 50
4.2.2 Courts 51
4.3 Reporting 51
4.3.1 Competent authorities 51
4.3.2 Contact details 52
4.3.3 Other reporting mechanisms 53
4.4 Forensics 57
4.4.1 Presentation of Documents 57
4.4.2 Presentation of Apparatus, Machines, Equipment – Physical Evidence 57
4.4.3 Evidence of Tapes, Recordings, Videos, etc 58
4.4.4 Hearsay Computer Evidence 58
4.4.5 Criminal Procedure 58
4.4.6 Arrest of a Person on Reasonable Suspicion of Having Committed an Offence 58
4.4.7 Search of Premises without a Warrant 59
4.4.8 Search of Premises with a Warrant (Anton Pillar Order) 59
4.4.9 Commencement of Criminal Proceedings 59
4.5 References 59

CHAPTER 5 **Country Report: Czech Republic 61**
5.1 Czech legislation on computer crimes 61
5.2 Law enforcement bodies 64
5.2.1 Police (www.mvcr.cz/2003/policie.html) 64
5.2.2 Courts (www.nsoud.cz/en/index.html and www.justice.cz) 64
5.2.3 Office for Personal Data Protection (www.uoou.cz) 65
5.3 Reporting 65
5.3.1 Competent authorities 65
5.3.2 Contact details 65
5.3.3 Other reporting mechanisms 66
5.4 Forensics 67
5.4.1 Obligation to yield an object 67
5.4.2 Interception and recording of telecommunication traffic 67
5.4.3 Involvement of experts 68
5.5 References (www.sbirka.cz) 68

CHAPTER 6 **Country report - Denmark 69**
6.1 Danish legislation on computer crimes 69

6.2 Law enforcement bodies 76
6.2.1 Police (www.politiet.dk) 76
6.2.2 Courts (www.cass.be) 76
6.3 Reporting 77
6.3.1 Competent authorities 77
6.3.2 Contact details 77
6.3.3 Other reporting mechanisms 77
6.4 Forensics 77
6.5 References (www.retsinfo.dk) 78

CHAPTER 7 **Country report - Estonia 79**
7.1 Estonian legislation on computer crimes 79
7.2 Law enforcement bodies 84
7.2.1 Police (www.pol.ee) 84
7.2.2 Courts (www.kohus.ee) 86
7.3 Reporting 86
7.3.1 Competent authorities 86
7.3.2 Contact details 86
7.3.3 Other reporting mechanisms 87
7.4 Forensics 87
7.4.1 Data seizure 88
7.4.2 Network searching 88
7.4.3 Involvement of experts 88
7.4.4 Internet monitoring 89
7.5 References (www.riigiteataja.ee) 89

CHAPTER 8 **Country Report: Finland 90**
8.1 Finnish legislation on computer crimes 90
8.2 Law enforcement bodies 98
8.2.1 Police (www.poliisi.fi) 98
8.2.2 Courts (www.oikeus.fi) 98
8.3 Reporting 99
8.3.1 Competent authorities 99
8.3.2 Contact details 99
8.3.3 Other reporting mechanisms 99
8.4 Forensics (www.oikeus.fi) 100
8.4.1 Disclosure of data 101
8.4.2 Telecommunications interception and monitoring 101
8.4.3 Restraint on alienation and seizure for escrow 101
8.5 References (www.om.fi, www.finlex.fi) 101

CHAPTER 9 **Country Report: France 102**
9.1 French legislation on computer crimes 102
9.2 Law enforcement bodies 105
9.2.1 Police (www.interieur.gouv.fr/rubriques/c/c3_police_nationale) 105

9.2.2 Courts (www.legifrance.gouv.fr) 106
9.3 Reporting 106
9.3.1 Competent authorities 106
9.3.2 Contact details 107
9.3.3 Other reporting mechanisms 107
9.4 Forensics 108
9.4.1 Search and seizure 108
9.4.2 Ordering the interception of communication 108
9.4.3 Ordering the participation of experts 109
9.4.4 Ordering the decryption of information 109
9.5 References (http://www.legifrance.gouv.fr/) 109

CHAPTER 10 **Country Report: Germany 110**
10.1 German legislation on computer crimes 110
10.2 Law enforcement bodies 113
10.2.1 Police (www.polizei.de) 113
10.2.2 Courts 114
10.3 Reporting 114
10.3.1 Competent authorities 114
10.3.2 Contact details 114
10.3.3 Other reporting mechanisms 114
10.4 Forensics 115
10.4.1 Data seizure 115
10.4.2 Network searching 116
10.4.3 Monitoring of e-mail traffic 116
10.4.4 Involvement of experts 116
10.5 References (http://bundesrecht.juris.de/bundesrecht/gesamt_index.html) 116

CHAPTER 11 **Country report - Greece 118**
11.1 Greek legislation on computer crimes 118
11.2 Law enforcement bodies 123
11.2.1 Police (www.ydt.gr) 123
11.2.2 Courts (www.ministryofjustice.gr/) 123
11.3 Reporting 124
11.3.1 Competent authorities 124
11.3.2 Contact details 124
11.3.3 Other reporting mechanisms 124
11.4 Forensics 124
11.5 References 125

CHAPTER 12 **Country report – Hungary 126**
12.1 Hungarian legislation on computer crimes 126
12.2 Law enforcement bodies 129
12.2.1 Police (http://web.b-m.hu/police/index.html) 129

12.2.2 Hungarian Customs and Finance Guard (http://vam.gov.hu/welcomeEn.do) 130
12.2.3 The Prosecutors Service (http://www.mklu.hu/cgi-bin/index.pl?lang=en) 130
12.2.4 Courts (http://www.birosag.hu) 131
12.3 Reporting 131
12.3.1 Competent authorities 131
12.3.2 Contact details 131
12.3.3 Other reporting mechanisms 132
12.4 Forensics 132
12.4.1 Data seizure 133
12.4.2 Network searching 133
12.4.3 Involvement of experts 133
12.5 References 134

CHAPTER 13 **Country report - Ireland 135**
13.1 Irish legislation on computer crimes 135
13.2 Law enforcement bodies 138
13.2.1 Police (www.garda.ie/angarda/gbfi.html) 138
13.2.2 Courts (www.attorneygeneral.ie) 139
13.3 Reporting 139
13.3.1 Competent authorities 139
13.3.2 Contact details 139
13.3.3 Other reporting mechanisms 139
13.4 Forensics 140
13.5 References (www.irlgov.ie) 140

CHAPTER 14 **Country Report: Italy 141**
14.1 Italian legislation on computer crimes 141
14.1.1 Specific legislation 141
14.1.2 Privacy Code 145
14.2 Law enforcement bodies 149
14.2.1 Police (www.poliziadistato.it) 149
14.2.2 Courts (www.cortedicassazione.it/) 150
14.3 Reporting 150
14.3.1 Competent authorities 150
14.3.2 Contact details 150
14.3.3 Other reporting mechanisms 150
14.4 Forensics 151
14.5 References 152
14.5.1 Particular cyber-crimes: 153
14.5.2 Forensics: 153

CHAPTER 15 **Country Report: Latvia 154**
15.1 Latvian legislation on computer crimes 154

15.2 Law enforcement bodies 158
15.2.1 State Police (http://www.vp.gov.lv/) 158
15.2.2 Courts (http://www.tiesas.lv/eng/) 159
15.3 Reporting 159
15.3.1 Competent authorities 159
15.3.2 Contact details 159
15.3.3 Other reporting mechanisms 160
15.4 Forensics 160
15.5 References (www.likumi.lv;www.ttc.lv/?id=50) 161

CHAPTER 16 **Country report - Lithuania 162**
16.1 Lithuanian legislation on computer crimes 162
16.2 Law enforcement bodies 166
16.2.1 Police (www.policija.lt) 167
16.2.2 Courts (www.teismai.lt) 167
16.2.3 Other institutions 167
16.3 Reporting 168
16.3.1 Competent authorities 168
16.3.2 Contact details 170
16.3.3 Other reporting mechanisms 170
16.4 Forensics 171
16.5 References (www.lrs.lt) 171

CHAPTER 17 **Country Report: Luxembourg 173**
17.1 Luxembourg legislation on computer crimes 173
17.2 Law enforcement bodies 175
17.2.1 Police (www.police.public.lu) 175
17.2.2 Courts 175
17.3 Reporting 176
17.3.1 Competent authorities 176
17.3.2 Contact details 176
17.3.3 Other reporting mechanisms 176
17.4 Forensics 176
17.5 References (www.legilux.public.lu) 177

CHAPTER 18 **Country report - Malta 178**
18.1 Maltese legislation on computer crimes 178
18.2 Law enforcement bodies 188
18.2.1 Police and Security Service (www.pulizija.gov.mt) 188
18.2.2 Courts 188
18.3 Reporting 189
18.3.1 Competent authorities 189
18.3.2 Other reporting mechanisms 189
18.4 Forensics 190
18.5 References (www.justice.gov.mt) 191

CHAPTER 19 **Country Report: The Netherlands** **192**
19.1 Dutch legislation on computer crimes 192
19.2 Law enforcement bodies 199
19.2.1 Police (www.politie.nl) 199
19.2.2 Courts (www.rechtspraak.nl) 199
19.3 Reporting 199
19.3.1 Competent authorities 199
19.3.2 Contact details 199
19.3.3 Other reporting mechanisms 200
19.4 Forensics 201
19.4.1 Data seizure 201
19.4.2 Subscriber data 201
19.4.3 Production orders 202
19.4.4 Network searching 202
19.5 References (www.wetten.nl) 202

CHAPTER 20 **Country Report: Poland** **203**
20.1 Polish legislation on computer crimes 203
20.2 Law enforcement bodies 206
20.2.1 Police www.kgp.gov.pl 206
20.2.2 Prosecution (www.ms.gov.pl/prokuratura) 207
20.2.3 Courts www.ms.gov.pl/sady 207
20.3 Reporting 208
20.3.1 Competent authorities 208
20.3.2 Contact details 208
20.3.3 Other reporting mechanisms 209
20.4 Evidence 210
20.5 References 211

CHAPTER 21 **Country report - Portugal** **212**
21.1 Portuguese legislation on computer related crimes 212
21.2 Law enforcement bodies 217
21.2.1 Police (www.pj.pt) 217
21.2.2 Courts 217
21.3 Reporting 218
21.3.1 Competent authorities 218
21.3.2 Contact details 218
21.3.3 Other reporting mechanisms 218
21.4 Forensics 219
21.4.1 House searching and seizure 219
21.4.2 Data seizure 219
21.4.3 Network searching 220
21.4.4 Involvement of experts 220
21.5 References 220

CHAPTER 22 **Country report – Slovak Republic** **221**
22.1 Slovak legislation on computer crimes 221
22.2 Law enforcement bodies 229
22.2.1 Police (www.minv.sk) 229
22.2.2 Office of the Public Prosecution (*Generálna prokuratúra Slovenskej republiky*) (www.genpro.gov.sk) 230
22.2.3 Courts (www.justice.gov.sk) 230
22.2.4 Office for Personal Data Protection (www.statnydozor@pdp.gov.sk) 231
22.3 Reporting 231
22.3.1 Competent authorities 231
22.3.2 Contact details 232
22.3.3 Other reporting mechanisms 232
22.4 Forensics 233
22.4.1 Obligation to yield an object 234
22.4.2 Seizure of an object 234
22.4.3 Domiciliary and personal search, search of other areas and estates, admittance to the dwelling, other areas and estates 234
22.4.4 Interception and recording of telecommunications traffic 234
22.4.5 Expert involvement 234
22.5 References (www.just.fgov.be) 235

CHAPTER 23 **Country report - Slovenia** **236**
23.1 Slovenian legislation on computer crimes 236
23.2 Law enforcement bodies 239
23.2.1 Police (www.policija.si) 239
23.2.2 Courts (www.sodisce.si) 239
23.3 Reporting 239
23.3.1 Competent authorities 239
23.3.2 Contact details 240
23.3.3 Other reporting mechanisms 240
23.4 Forensics 241
23.5 References 241

CHAPTER 24 **Country report - Spain** **242**
24.1 Spanish legislation on computer crimes 242
24.2 Law enforcement bodies 250
24.2.1 Police (www.policia.es) 250
24.2.2 Guardia Civil (www.guardiacivil.org) 250
24.2.3 Courts (www.poderjudicial.es) 250
24.3 Reporting 250
24.3.1 Other reporting mechanisms 251
24.4 Forensics 252
24.4.1 Data seizure 252
24.4.2 Network searching 253

24.5 References 253

CHAPTER 25 **Country report - Sweden 254**
25.1 Swedish legislation on computer crimes 254
25.2 Law enforcement bodies 256
25.2.1 Police (www.polisen.se) 256
25.2.2 Courts (www.domstolsverket.se) 258
25.3 Reporting 258
25.3.1 Competent authorities 258
25.3.2 Contact details 258
25.3.3 Other reporting mechanisms 258
25.4 Forensics 259
25.5 References 259

CHAPTER 26 **Country Report - United Kingdom 261**
26.1 UK legislation on computer crimes 261
26.2 Law Enforcement Bodies 266
26.2.1 Police 266
26.2.2 Courts 266
26.3 Reporting 266
26.3.1 Competent Authorities 266
26.3.2 Contact Details 267
26.3.3 Other reporting mechanisms 267
26.4 Forensics 268
26.5 References 269

Executive Summary

This document represents one of the two main deliverables of the 2005 project to update the 2003 CSIRT Legal Handbook. It sets out in a concise form the legal status of different types of computer misuse under the legal systems of the EU countries. The study reviewed the information in the 2003 CSIRT Legal Handbook, which covered the 16 member states, and also included information relating to the new member states which joined in 2004. Information relating to the legal environment for dealing with cyber-crime in each member state was also accompanied by an indication of the prosecution policy of law enforcement agencies in the countries, along with standard rules or procedures for the collection, handling documentation and reporting of computer based evidence. Penal and civil law was considered where applicable.

The Country Reports section begins with an introduction to the supra-national legislative environment pertinent to cyber-crime. The chapters for each country are then presented alphabetically. They are kept concise to ensure brevity and usefulness for the user community. Each country chapter is split into the following sub-sections:

Legislation on Computer Crime
This sub-section presents a general overview of the extent and nature of computer crime legislation in the country. It details whether specific laws have been created to deal with computer crimes or whether these are covered under amendments to existing legislation (e.g. theft). It also highlights the existence of particular legislation to deal with spam or identity theft. This section also contains a table that indicates which penalty, under which law is applicable for a certain type of incident. The severity of the penalty is shown, as is the law under which it is prosecutable (known as applicable provision) and the legal description of the incident.

This sub-section also includes a table of incident types, along with the applicable legal provisions and the sanctions imposed in these provisions specifying the duration of imprisonment and the amount of the fines whenever possible. In order to obtain comparable results for all Member States, these incident types are fixed according to the taxonomy outlined earlier. In the rare event that no provisions apply to an incident, a note is simply made that there is "no applicable provision". Note that legal provisions can be criminal or administrative in nature. Both categories are included in the same table.

Also note that one incident can be covered by more than one provision and that one provision can apply to many incidents. Finally, it is even possible that one provision contains two or more different crimes with different sanctions.

Law Enforcement bodies

This sub-section indicates briefly which law enforcement organisations are present in the country, their structure, roles and estimated effectiveness. It also details the judicial system and what courts are most likely to deal with computer crime incidents and how the process works for appeals to a court of higher authority.

Reporting

This sub-section details the existence of reporting mechanisms in the country, including national schemes and non-national or voluntary activities.

Forensics

This sub-section details forensic procedures in common use in the country (for example, network searching and data seizure).

References

Finally, each chapter lists the references to the legal provisions themselves, including an English translation of the titles.

Country Reports

CHAPTER 1 Introduction to Country Reports

The following chapters reflect the collation and management of information submitted by country correspondents for each of the 25 MS. Lawfort were asked to undertake a national legal survey of cyber-crime law in the Member States. To do this they contacted an extensive network of correspondents in each country and asked them to submit information according to a standard country chapter template. The sources themselves come from a wide variety of backgrounds: academics, lawyers, national CSIRT representatives, magistrates, and security consultants.[1]

These correspondents were also asked to detail what laws would be relevant to the defined list of incidents, contained in the previously developed taxonomy.

Using country correspondents has two advantages. Firstly the information has a greater chance of being up to date and accurate, as those responsible for dealing with cyber-crime (either due to their role as lawyers, technical experts or law enforcement representatives) out of necessity must keep up to date with the latest developments. Secondly, the country correspondents, because of the familiarity with the national legal system, will be best placed to know which laws can be applied to which incidents.

In addition being asked to submit a variety of information relating to the legislative background, law enforcement organisations, reporting mechanisms and evidential procedures concerning cyber-crime in each country, correspondents were asked to fill in a table detailing which national laws were relevant to the defined taxonomy of incidents.

1.1 Taxonomy of Information Security Incidents

The following list describes and defines a taxonomy or classification of Information Security Incidents that the country correspondents were asked to relate to laws in their own country.

Target Fingerprinting
This can be usually defined as actions performed in order to gather information about a target by directly communicating with the target itself

[1] The information for Belgium, France, Ireland, the Netherlands and the UK was principally collected by RAND Europe and/or Lawfort.

Unauthorised Access to Transmissions
This can be generally defined as interfering without right and by technical means, with non-public transmissions of computer data to, from, or within a computer system. Intercepting network packets, injecting packets into traffic flow and removing packets from traffic flow are all means of undertaking this incident.

Unauthorised Access to Information
This is generally defined as attempts to obtain unauthorised access to data and can be accomplished by trying to gain access, either locally or remotely, to data circumventing access control mechanisms.

Unauthorised Modification of Data
This can be usually defined as the unauthorised modification of information that is held electronically on a computer system. Methods of conducting this are by local or remote modification, or creation of any kind of data, which resides in a computer without the required authorisation.

Malicious Code
This is usually defined as the compromise of a target host via independent program execution. This can be undertaken via conscious or unconscious independent program execution.

Denial of Service
Denial of service can be generally defined as repeated target access that overloads capacity or otherwise disrupts a service. It is usually conducted via the execution of programs which perform endless requests of computer resources such as: memory, CPU time, TCP–UDP connections, disk space.

Account Compromise
This is usually defined as unauthorised access to a system, or system resource at sys-admin ('root' or 'admin') level or user level. This is usually executed via the exploitation, either locally or remotely, of software vulnerabilities in order to obtain unauthorised access to user accounts. However, the same result can also be obtained using credentials which have been illegally obtained (stolen, intercepted, coerced).

Intrusion attempt
Attempted unauthorised access to a computer system. This is accomplished either via trying to gain access to a system by guessing users' credentials, or unsuccessfully trying to perform any of the following methods: multiple login attempts; unsuccessful buffer overflow attempts; use of default user ID/password; attempts to exploit older vulnerabilities; attempted use of default accounts; attempted connections to SMNP ports.

Unauthorised Access to Communications Systems
The unauthorised remote access to a computer connected to a network or a telecommunication system. This can usually be accomplished via network penetration or interference with network connection equipment.

Spam
The distribution of unsolicited commercial messages without consent or heed to the recipients' wishes to receive such messages. This is usually undertaken by the distribution (often automated) of email messages, without a message or opportunity to unsubscribe (or where there is one, it does not function).

1.2 The Criminality of Incidents across the EU

Table 1 provides an overview of the sanctions that the 25 Member States have legislated for the incident types surveyed as a part of the 2005 CSIRT Legal Handbook. It also indicates if the provided sanction has an administrative or penal character. In some cases, both a penal and an administrative sanction may apply; this is marked in the table as "crim+adm".

Occasionally, an incident may not be punishable as such, although it could be qualified as a punishable act depending on the circumstances. The most common example is Target Fingerprinting: while most states do not consider fingerprinting to be punishable as such, it can often be interpreted as a preparatory act in view of committing a different crime, e.g. unauthorised access. Such cases are indicated as "n.a.s." (not as such) in the table above. We refer to the country reports for a more detailed explanation of each separate case.

Note that the table above only includes the status of Member States for which a final status report is available at the time of writing (29 June 2005). When a country report has not yet been received, or when it has not yet undergone a quality review, then the Member State's status is marked as "unav." (unavailable). This is currently the case for Austria, Ireland, Slovakia and Sweden. All of these reports are scheduled to be completed in the following few days, and the status of these Member States will be added in the final version of the table in the CSIRT Handbook.

Table 1: Overview of Criminality of Incidents across the 25 MS

Country	Target Fingerprinting	Malicious Code	Denial of service	Account compromise	Intrusion attempt	Unauthorised access to information	Unauthorised access to transmissions	Unauthorised modification of information	Unauthorised access to communication systems	Spam
Austria	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
Belgium	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
Cyprus	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim+ adm
Czech	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim + adm
Denmark	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim + adm
Estonia	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
Finland	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
France	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim + adm
Germany	n.a.s.	n.a.s.	crim.	n.a.s.	n.a.s.	crim.	crim.	crim.	crim.	n.a.s.
Greece	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	n.a.s.
Hungary	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	adm.
Ireland	n.a.s.	crim.	crim.	adm.	Adm.	crim + adm	n.a.s.	n.a.s.	crim + adm.	adm.
Italy	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
Latvia	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	n.a.s.
Lithuania	n.a.s.	crim+ adm	crim.	crim.	crim	crim	crim	crim.	crim	adm.
Luxemburg	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
Malta	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	adm.
Poland	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
Portugal	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	adm.
Slovakia	n.a.s.	crim	crim	crim.	crim	crim	crim	crim	crim.	crim + adm.
Slovenia	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.
Spain	n.a.s.	crim.	crim.	n.a.s.	n.a.s.	crim.	crim.	crim.	crim.	crim.
Sweden	crim.	crim.	crim.	crim.	crim.	crim.	crim	crim.	crim	adm.
The Netherlands	n.a.s.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	crim.	adm.
United Kingdom	crim.	crim.	crim.	crim.	crim	n.a.s	crim	crim	crim	adm.

Legend	
n.a.s.	Not as such, i.e. there is no provision covering this act autonomously, but depending on the circumstances of the act, it may be classifiable as a different form of crime or an attempt to commit such a crime. See the country report for specific details.
crim.	A penal sanction is provided.
adm.	An administrative sanction is provided.

1.3 Matching incidents to the Framework Decision and Council of Europe Cyber-Crime Convention

In international terms, the Council of Europe's Convention on Cybercrime is considered to be one of the main unique points of reference. The final text was agreed on 23 November 2001, and the Convention is open for signature by CoE Member States and those non-Member States that participated in its elaboration (including Canada, Japan, and the USA). Additionally, it is open for accession by other non-Member States. The Convention is one of the most comprehensive documents on cyber-crime available. It contains concrete efforts towards the outlining of common definitions for crimes related to computer systems, as well as a series of measures encouraging international cooperation.

Although the Convention was drafted in 2001, it did not enter into force until 1 July 2004[2]. A further Protocol was signed on 28 January 2003 but has not yet entered into force[3]. The Handbook legal survey was conducted taking into account the legal definitions provided by the Convention on Cybercrime.

In addition to this initiative of the Council of Europe, the European Council Framework Decision on Attacks against Information Systems on 24 February 2005 was adopted. The objective of this initiative is 'to improve cooperation between judicial and other competent authorities, through approximating rules on criminal law in the Member States in the area of attacks against information systems'. As explained in the Framework Decision, attacks against information and computer systems are a concrete and dangerous threat that requires an effective response. Specifically, it is necessary to further increase awareness of the problems related to information security and to provide practical assistance.

This Framework Decision intends to complement the work performed by international organisations, in particular that of the Convention on Cybercrime. As a consequence, it should come as no surprise that the Convention and the Framework Decision are closely connected and that their definitions are synchronised. This can be seen most clearly in the descriptions of three central criminal offences: illegal access to information systems (article 2), illegal system interference (article 3) and illegal data interference (article 4). These provisions closely resemble the Convention's illegal access (article 2), system interference (article 5) and data interference (article 4). Interestingly, the Convention's illegal interception provision (article 3) has no equivalent in the Framework Decision. Member States must now transpose the provisions of the Decision within two years.

---

[2] Due to its article 36, which contains the conditions for entry into force. It specifies that the Convention should first be ratified by five States, including three Member States of the Council of Europe. The Convention would then enter into force on the first day of the month following the expiration of a three month period after the fifth ratification. This condition was fulfilled with Lithuania's ratification on 18 March 2004, triggering the entry into force on 1 July 2004.

[3] Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No.: 189 at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=10/02/05&CL=ENG

Both the Convention and the Framework decision are concerned specifically with *offences against the confidentiality, integrity and availability of computer data and systems*. Table 2 below summarises the articles from the Convention and the Framework Decision, and allows the incident types of this Handbook to be matched to their corresponding provision in each international text. Note that this table should not be interpreted as a 1:1 mapping from incidents to Convention/Framework Decision: an incident can not always be qualified as the crimes indicated in the table below. Rather, the table indicates for each incident which qualification is likely, under the Convention or Framework Decision.

It is worth noting that the Convention and the Framework Decision also share a number of other provisions, including the legal consequences of aiding and abetting, and the liability of legal persons. Although they do not correspond with incident types, they are still included in the table below for ease of reference.

The Convention on Cybercrime, and Additional Protocol, also deals with a number of crimes that are not addressed by the Framework Decision, such as computer related forgery, computer related fraud, and content related offences. Although they can certainly be considered as a category of computer-related crime, they are not examined in detail within this Handbook, as they clearly concern crimes in which the involvement of computers can be characterised as a circumstance of the specific crime, rather than as an essential component of it. For example, child pornography (Article 9 of the Convention) can be spread and acquired with or without a computer; as such, the use of a computer is an aggravation of an existing offence, not a new offence entire of itself.

However, it is important to point out that Member State legislation may exist only for crimes that are perpetrated in the offline environment. These legislative measures may not be sufficiently adapted to be applied to similar crimes being perpetrated with the assistance of a computer.

Table 2: Incidents matched to the legal frameworks of the Council of Europe Cyber-crime Convention and the Council Framework Decision on attacks against information systems.

Handbook cyber-crime definition	Council of Europe Convention on Cybercrime	Council Decision on attacks against information systems
Target Fingerprinting Malicious Code Denial of Service Account Compromise Intrusion Attempt Unauthorised Access to Information Unauthorised Access to Transmissions Unauthorised Modification of Information Unauthorised Access to Communication Systems	Illegal access (Article 2): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	Illegal access to Information Systems (Article 2): 1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor. 2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminating only where the offence is committed by infringing a security measure.
Target Fingerprinting Malicious Code Unauthorised Access to Transmissions Unauthorised Access to Communication Systems	Illegal interception (Article 3): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	Not defined within the Framework Decision.
Malicious Code Intrusion Attempt Unauthorised Access to Information Unauthorised Modification of Information Unauthorised Access to Communication Systems	Data interference (Article 4): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	Illegal data interference (Article 4) Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.
Malicious Code Denial of Service Intrusion Attempt Unauthorised Access to Information Unauthorised Modification of Information Unauthorised Access to Communication Systems	System interference (Article 5): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	Illegal system interference (Article 3) Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at

		least for cases which are not minor.
Target Fingerprinting Malicious Code Denial of Service Intrusion Attempt Unauthorised Access to Transmissions Unauthorised Modification of Information Unauthorised Access to Communication Systems	Misuse of devices (Article 6): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2–5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and b. the possession of an item referred to in paragraphs (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1(a)(ii).	Not defined within the Framework Decision.

	Attempt and aiding or abetting (Article 11) 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention. 3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	Instigation, aiding and abetting and attempt (Article 5) 1. Each Member State shall ensure that the instigation of aiding and abetting an offence referred to in Articles 2, 3 and 4 is punishable as a criminal offence. 2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable as a criminal offence. 3. Each Member State may decide not to apply paragraph 2 for the offences referred to in Article 2.

	Corporate liability (Article 12) 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person. 2. Apart from the cases already provided for in paragraph 1, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	Liability of legal persons (Article 8) 1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: (a) a power of representation of the legal person, or (b) an authority to take decisions on behalf of the legal person, or (c) an authority to exercise control within the legal person. 2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority. 3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the commission of the offences referred to in Articles 2, 3, 4 and 5.
	Sanctions and measures (Article 13) 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or noncriminal sanctions or measures, including monetary sanctions.	Penalties (Article 6) 1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 2, 3, 4 and 5 are punishable by effective, proportional and dissuasive criminal penalties. 2. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 3 and 4 are punishable by criminal penalties of a maximum of at least between 1 and 3 years of imprisonment.

CHAPTER 2 Country Report - Austria

2.1 Austrian Legislation on Computer Crimes

In the course of implementing the Cyber-Crime-Convention an amendment to the Austrian Criminal Code (StGB)[4] entered info force on 1 October 2002 (BGBl. I 134/2002, *"Strafrechtsänderungsgesetz 2002"*). It introduced a few new specific computer crimes and amended some of the already existing sanctions regarding cyber crime. These are especially unlawful access to a computer-system (§ 118 a StGB), infringement of telecommunications secrecy (§ 119 StGB), interception of data (119 a StGB), damage of data and computer systems (§ 126 a StGB), abuse of software or access rights (§ 126 b StGB), fraudulent abuse of automated data processing (§ 148a StGB) and forgery of computer data (§ 225 a StGB).

Relevant Incidents	Applicable provision (see Note 1)	Description	Sanction
Computer Fingerprinting	None as such	Not punishable as long as no intrusion into a secured computer system is established according to § 118 a StGB	
Malicious Code	§ 118 a StGB	Unauthorised access to a computer system with intent to gain or damage	Imprisonment up to 6 months or fine up to 360 daily rates[5] (penal sanction)

[4] A list of the used abbreviations can be found in the list of the Austrian laws.

5 Penalties are computed in daily rates that are determined according to the crime and guilt of the lawbreaker (§ 19 StPO). The amount of a daily rate depends on the personal means and economic productivity of the delinquent (from EUR 2 to 500).

	§ 126 a StGB	Wilful act of data damage	Imprisonment up to 6 months or fine up to 360 daily rates; Qualification 1 (loss higher than EUR 3,000): imprisonment up to 6 years or fine up to 360 daily rates; Qualification 2 (loss higher than EUR 50,000): imprisonment between 6 months and 5 years (penal sanction)
		Depending on the results of the action, the realisation of various elements of other crimes is possible, in particular spying on personal data (§ 51 DSG), disruption of the operability of a computer (§ 126 b StGB), etc.	
Denial of Service	§ 126 b StGB	Disruption of the operability of a computer system	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
Account Compromise	§ 118 a StGB	Unauthorised access to a computer system with intent to gain or damage	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
	§ 126 c para. 1 no. 2 StGB	Abuse of access data	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
	§ 52 para. 1 no. 1 DSG	Unauthorised access to an application of personal data	Fine up to EUR 18,890 (administrative sanction)
	§ 10 ZuKG	Professional sale or rent of circumvention measures	Imprisonment up to 2 years or fine up to 360 daily rates (penal sanction)
	§ 13 ZuKG	Intentional and professional use of or advertisement for circumvention measures	Fine up to EUR 15,000 (administrative sanction)
	§ 26 SigG	Misuse of electronic signature creation data	Fine up to EUR 4,000 (administrative sanction)
Intrusion Attempt	§ 126 c para. 1 no. 2 StGB, §§ 10 and 13	Preparatory acts are covered by the elements of these	

	ZuKG	offences (see above)	
Unauthorised Access to Information	§ 118 a StGB	Unauthorised access to a computer system with intent to gain or damage	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
	§ 13 ZuKG	Intentional and professional use of or advertisement for circumvention measures	Fine up to EUR 15,000 (administrative sanction)
	§ 51 DSG	Use of personal data with intent to gain or damage	Imprisonment up to 1 year (penal sanction)
	§ 52 para. 1 no. 1 DSG	Unauthorised access to an application of personal data	Fine up to EUR 18,890 (administrative sanction)
	§ 123 StGB	Exploitation of business or company secrets	Imprisonment up to 2 years, fine up to 360 daily rates (penal sanction, private accusation required)
Unauthorised Access to Transmissions	§ 119 a StGB	Abusive interception of data	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
	§ 119 StGB	Violation of the secrecy of telecommunication	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
	§ 120 para. 2a StGB	Abusive use of communication (e.g. e-mail)	Imprisonment up to 3 months or fine up to 180 daily rates (penal sanction)
		Depending on the results of the action the realisation of various other offences is possible, in particular §§ 51, 52 DSG, § 123 StGB, etc.	
Unauthorised Modification of Information	§ 126 a StGB	Wilful act of data damage	Imprisonment up to 6 months or fine up to 360 daily rates; Qualification 1 (loss higher than EUR 3,000): imprisonment up to 6 years or fine up to 360 daily rates; Qualification 2 (loss higher than EUR 50,000): imprisonment between 6 months and 5 years (penal sanction)

	§ 148 a StGB	Fraudulent abuse of data processing	Imprisonment up to 6 months or fine up to 360 daily rates; Qualification 1 (professional commitment or loss higher than EUR 3,000): imprisonment up to 3 years Qualification 2 (loss higher than EUR 50,000): imprisonment between 1 and 10 years (penal sanction)
	§ 225 a StGB	Forging of data	Imprisonment up to 1 year (penal sanction)
		Depending on the results of the action, the realisation of various offences is possible, in particular forgery of documents (§ 223 StGB), fraud (§ 146 StGB), etc.	
Unauthorised access to communication systems	§ 119 StGB	Violation of the secrecy of telecommunication	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
	§ 93 in conjunction with § 108 TKG	Violation of the secrecy of communication (communication provider)	Imprisonment up to 3 months or fine up to 180 daily rates (penal sanction)
	§ 119 a StGB	Abusive interception of data	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)
	§ 120 para. 2a StGB	Abusive use of communication (e.g. e-mail)	Imprisonment up to 3 months or fine up to 180 daily rates (penal sanction)
		Eventually also unauthorised access to a computer system (§ 118 a StGB), abusive use of communication (§ 120 StGB), etc.	
Spam	§ 107 para. 2 in conjunction with § 109 para. 3 no. 19-21 TKG	Unsolicited e-mails (except in case of business contacts)	Fine up to EUR 37,000 (administrative sanction)

	§ 126 b StGB	Disruption of the operability of a computer system (by transmission)	Imprisonment up to 6 months or fine up to 360 daily rates (penal sanction)

Note 1: An amendment to the Austrian Criminal Code, which entered into force on 1 May 2004 (BGBl. I 15/2004, *"Strafrechtsänderungsgesetz 2004"*), reorganised in particular sexual offences (especially child pornography, § 207 a StGB) and offences regarding non-cash means of payment (§§ 241 a – g StGB).

Furthermore there are several related provisions in different laws, in particular within the Austrian Data Protection Act (secrecy of personal data, §§ 1, 15 DSG; administrative penalties regarding secrecy and security of personal data, § 52 DSG; use of personal data with intent to gain or damage, § 51 DSG), the Austrian Telecommunications Act (duty of disclosure, § 90 Abs 6 TKG; communications secrecy, § 93 TKG; spamming, § 107 TKG; data secrecy, §§ 96 - 99 TKG; sanctions §§ 108 - 111 TKG), the Austrian Media Act (media contents offences, § 28 MedienG), the Austrian E-Commerce Act (provider liability, §§ 13 – 19 ECG; spamming, §§ 6 - 7 ECG in conjunction with § 26 ECG; duty of disclosure, § 18 ECG), the Austrian Copyright Act (protection of software, technical measures and labelling, §§ 90 b – d in conjunction with § 91 UrhG), Austrian Access Control Law (§ 10 ZuKG) or the Austrian Digital Signature Act (misuse of private encryption keys, § 26 SigG).

Moreover, "common offences" can be committed or supported by the use of computers, in particular disseminating banned contents on the Internet (liable to prosecution are e.g. the so-called "Nazi offences" *(NS Delikte)* accordingto § 3 h VerbotsG, child pornography according to § 207 a StGB), fraud (§ 146 StGB) or blackmail (§ 144 StGB).

2.2 Law Enforcement Bodies

2.2.1 Police (www.polizei.gv.at)

Austrian police consists of the federal police *(Bundespolizei)* and some local police units engaged in community policing. Beside two specialised units the enforcement of cyber-crime offences is handled by the regional crime units. The police investigation is supervised and guided by district authorities and – in case of criminal offences – by public prosecutors. District authorities, Federal Police Head Offices, public prosecutors or courts may initiate their own investigation procedures.

2.2.2 Austrian Administrative Adjudication

The administrative penalty procedure proceeds before an administrative authority. District authorities ("*Bezirksverwaltungsbehörden*") and the Federal Police Head Offices ("*Bundespolizeidirektionen*") are - within their respective areas of competence – authorities of first instance. Independent tribunals ("*Unabhängige Verwaltunssenate*") are the competent authorities of second instance which handle appeals against the authorities of first instance. The administrative decisions may be reviewed by the Administrative Court ("*Verwaltungsgerichtshof*"); in constitutional matters (e.g. human rights) the Constitutional Court ("*Verfassungsgerichtshof*" has the exclusive competence.

The procedure is ruled by the Austrian Administrative Procedure Act (AVG) and the Austrian Administrative Penalty Act (VStG). In Austrian administrative adjudication both fines and prison sentences may be imposed.

2.2.3 Austrian Criminal Proceedings

Austrian criminal law distinguishes, depending on the penalty, between felony ("*Verbrechen*") and misdemeanour ("*Vergehen*"). Felonies are all offences threatened by a term of imprisonment of more than three years, all the other offences are classified as misdemeanours.

The District Courts ("*Bezirksgerichte*") generally exercise jurisdiction regarding all misdemeanours punished by not more than one year of imprisonment. The Regional Courts ("*Landesgerichte*") exercise jurisdiction for all the other offences and act as courts of appeal in respect to the decisions of the District Courts. The Courts of Appeal ("*Oberlandesgerichte*") function as appellate courts for the Regional Courts. The Supreme Court ("*Oberster Gerichtshof*") hears nullity appeals. The Austrian code of criminal procedure (StPO) restricts the procedure to one level of appeal.

The investigation of crimes is conducted by public prosecutors with the support of the federal police under the supervision of courts.

2.3 Reporting

2.3.1 Competent Authorities

In all cases of computer crime, the federal police, the public prosecutors, the district authorities or courts may be alerted. Child pornography[6] and the so-called "Nazi offences" [7] should be reported to the special information units.

2.3.2 Contact Details

Internet users and ISP's can notify any supposed offence of child pornography on the Internet to the *Meldestelle Kinderpornografie* (Reporting Office for Child Pornography). Notifications can be made on an anonymous basis and should contain as much useful information as possible, such as the URL of the website and the full heading of a news item.

Bundesministerium für Inneres (Austrian Federal Ministry of the Interior)
Generaldirektion für die öffentliche Sicherheit (Directorate-General for Public Security)
Bundeskriminalamt (Federal Criminal Office)
Meldestelle Kinderpornographie
Josef Holaubek Platz 1
A-1090 Wien
Tel: +43 (0)1 53126-0
Fax: +43 (0)1 31345-85190
meldestelle@interpol.at

Internet users and ISP's can notify any supposed offence of the so-called "nazi offences" on Internet to the *Meldestelle für NS-Wiederbetätigung* (Reporting Office for Nazi Activities). Notifications can be made on an anonymous basis and should contain as much useful information as possible, such as the URL of the website and the full heading of a news item.

---

[6] § 207 a StGB: Sanctioned by imprisonment up to 3 years; in case of aggravated circumstances (professional commitment), the punishment is raised to imprisonment between 6 months and 5 years; in case of further aggravated circumstances (brute force, criminal ring, etc.), the punishment is raised to imprisonment between 1 and 10 years. In case of mere purchasing or possession of child pornography, the penalty is imprisonment up to 2 years (penal sanction).

[7] § 3 h VerbotsG: Sanctioned by imprisonment between 1 and 10 years; in case of aggravated circumstances (high degree of danger), the punishment is raised to imprisonment between 1 and 20 years (penal sanction)

Bundesministerium für Inneres
Generaldirektion für die öffentliche Sicherheit
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Federal Office for the Protection of the Constitution and Combating Terrorism)
Meldestelle für NS-Wiederbetätigung
Herrengasse 7
A-1014 Wien
Tel: +43 (0)1 53126-0
ns-wiederbetaetigung@mail.bmi.gv.at

According to § 7 Abs 2 ECG the *Rundfunk und Telekom Regulierungs-GmbH* (RTR-GmbH) (Austrian Regulatory Authority for Broadcasting and Telecommunications) must keep a list in which the persons and companies not desiring to receive commercial communications by electronic mail can be entered free of charge. Service providers must comply with the list:

Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77-79
A-1060 Wien
Phone: +43 (0)1 58058–0
Fax: +43 (0)1 58058-9191
rtr@rtr.at

For criminal offences concerning child pornography and the so-called „Nazi offences" the ISPA (Internet Service Providers Austria) has set up a reporting unit: http://hotline.ispa.at, e-mail: meldung@stopline.at. A report can be submitted on an anonymous basis.

2.4 Forensics

The investigation of crimes is conducted by public prosecutors with the support of the federal police under the supervision of courts.

Confiscation of computers or parts of a computer system may be ordered by a court (§§ 143 – 149 StPO). This interference is only allowed to the extent required and the least harmful means have to be used (e.g. a copy of a hard disk may be left to the third party or accused person). Telephone surveillance is possible under certain conditions (149 a – c StPO). A general duty to provide information exists for criminal offences (§ 149 a StPO); a special one for internet providers (§ 18 ECG).

Involvement of expert evidence is not very common. The police is responsible for conducting investigations, and typically that is sufficient.

2.5 References

Bibliography

- Ebensperger, S.: *Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen*, ÖJZ 2002, 132.
- Freund, W.: *Die Strafbarkeit von Internet Delikten*, Wien 1998.
- Handig, C.: *Das Herkunftslandprinzip und seine Auswirkungen in den verschiedenen Rechtsbereichen*, wbl 2003, 253.
- Himberger, S.: *Fernmeldegeheimnis und Überwachung*, Neuer Wissenschaftlicher Verlag, Wien 2004.
- Maleczky, O.: *Das Strafrechtsänderungsgesetz 2002*, JAP 2002/2003, 115.
- Maleczky, O.: *Das Strafrechtsänderungsgesetz 2004*, JAP 2003/2004, 250.
- Plöckinger, O./Duursma, D. /Mayrhofer, M.: (Eds.): *Internet-Recht*, Neuer Wissenschaftlicher Verlag, Wien 2004.
- Plöckinger, O.: *Die neuen Tatbestände zum Schutz unbarer Zahlungsmittel und deren Verhältnis zu den Urkunden- und Vermögensdelikten*, ÖJZ 2005, 14.
- Plöckinger, O.: *Zur Zuständigkeit österreichischer Gerichte bei Straftaten im Internet*, ÖJZ 2001, 798.
- Reindl, S.: *Computerstrafrecht im Überblick*, WUV-Verlag, Wien 2004.
- Reindl, S.: *E-Commerce und Strafrecht*, Neuer Wissenschaftlicher Verlag, Wien 2003.
- Schweighofer, E.: *Neue Medien und Gewalt: die Rechtssituation*, in: CD Austria, Sonderheft 11/2002 des bm:bwk, Gewalt und Medien, 13-15.

Relevant Laws

The Austrian Federal Chancellery provides free access to Austrian laws on the Internet. A selection of important Austrian laws is also offered in English:

http://www.ris.bka.gv.at/

- AVG: Allgemeines Verwaltungsverfahrensgesetz 1991, Austrian Administrative Procedure Act, BGBl. (Federal Gazette) 51/1991, as lastly amended BGBl. I 10/2004
- DSG: Datenschutzgesetz 2000, Austrian Data Protection Act, BGBl. I 165/1999, as lastly amended BGBl. I 13/2005
- ECG: E-Commerce-Gesetz Austrian E-Commerce Act, BGBl. I 152/2001
- MedienG: Mediengesetz, Austrian Media Act, BGBl. 314/1981, as lastly amended BGBl. I 49/2005
- SigG: Signaturgesetz, Austrian Digital Signature Act, BGBl. I 190/1991, as lastly amended BGBl. I 152/2001

- StGB: Strafgesetzbuch, Austrian Criminal Code, BGBl. 60/1974, as lastly amended BGBl. I 152/2004
- StPO: Strafprozessordnung 1975, Austrian Code of Criminal Procedure, BGBl. 631/1975, as lastly amended BGBl. I 164/2004
- TKG: Telekommunikationsgesetz 2003, Austrian Telecommunications Act, BGBl. 70/2003, as lastly amended BGBl. 178/2004
- UrhG: Urheberrechtsgesetz, Austrian Copyright Act, BGBl. 111/1936, as lastly amended BGBl. I 32/2003
- VerbotsG, Verbotsgesetz 1947, Nazi Offences Act, StGBl (State Gazette) 13/1945 as amended by Federal Gazette 25/1947, lastly amended BGBl. I 148/1992
- VStG: Verwaltungsstrafgesetz 1991, Austrian Administrative Penalty Act, BGBl. 52/1991, as lastly amended BGBl. I 117/2002
- ZuKG: Zugangskontrollgesetz, Austrian Access Control Law, BGBl. I Nr. 60/2000, as lastly amended BGBl. I 32/2001

CHAPTER 3 Country Report: Belgium

3.1 Belgian legislation on computer crimes

For cases where traditional crimes and investigation measures can not sufficiently deal with offences against the Confidentiality Integrity and Availability of offences, a law of 28 November 2000 introduced four specific computer crimes (informatics forgery, informatics fraud, data manipulation and hacking), three specific investigation measures (data seizure, network searching and expert involvement) and a provision imposing data retention obligations on operators and service providers of electronic communication. This provision has not yet entered into force because Belgium is awaiting the outcome of discussions at European level, where a period between 12 and 36 months has been suggested for data retention

In addition, specific laws penalise spam, the interference with military communications to hinder their functioning and the unauthorised deliberate access to the national social security database.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Article 314*bis* Criminal Code	Interception of private communication or data communication without the agreement of all parties involved	Imprisonment of 1 year (2 years if the offender is a government officer) and/or a fine up to EUR 50,000
Malicious code	Article 210*bis* Criminal Code	Changing or deleting electronic data so that their legal scope changes and the deliberate use of such data	Imprisonment between 6 months and 5 years and/or a fine up to EUR 500,000. Attempts are subject to imprisonment between 6 months and 3 years and a fine up to EUR 250,000.
	Article 550*bis* Criminal Code	The (even unintentional) causing of damage to a computer system or to data stored on, processed or transmitted by such a system after unauthorised access thereto	Imprisonment between 1 and 3 years and/or a fine up to EUR 250,000
Denial of service	Article 210*bis* Criminal Code	Changing or deleting electronic data so that their legal scope changes and the deliberate use of such data	Imprisonment between 6 months and 5 years and/or a fine up to EUR 500,000. Attempts are subject to imprisonment between 6 months and 3 years and a fine up to EUR 250,000.
Account compromise	Article 550*bis* Criminal Code	Unauthorised access and maintenance of access to a computer system (outsiders), even with no intention to cause harm	Imprisonment between three months and one year (two years in case of intent) and/or a fine up to EUR 125,000
Intrusion attempt	Article 550*bis* Criminal Code	Preparatory measures in view of unauthorised access	Imprisonment between 6 months and 3 years and/or with a fine up to EUR 500,000
Unauthorised access to information	Article 550*bis* Criminal Code	Unauthorised access and maintenance of access to a computer system even with no intention to cause harm	Imprisonment between three months and one year (two years in case of intent) and/or a fine up to EUR 125,000
		Intentional abuse of access rights by an authorised user of a computer system	Imprisonment between 6 months and 2 years and/or a fine up to EUR 125,000

	Article 314*bis* Criminal Code	Interception of private communication or data communication without the agreement of all parties involved	Imprisonment of 1 year (2 years if the offender is a government officer) and/or a fine up to EUR 50,000
Unauthorised access to transmissions	Article 314*bis* Criminal Code	Interception of private communication or data communication without the agreement of all parties involved	Imprisonment of 1 year (2 years if the offender is a government officer) and/or a fine up to EUR 50,000
		Disclosure of the contents of intercepted communication	Imprisonment between 6 months and 2 years and/or a fine up to EUR 100,000.
Unauthorised modification of information	Article 210*bis* Criminal Code	Changing or deleting electronic data so that their legal scope changes and the deliberate use of such data	Imprisonment between 6 months and 5 years and/or a fine up to EUR 500,000. Attempts are subject to imprisonment between 6 months and 3 years and a fine up to EUR 250,000.
Unauthorised access to communication systems	Article 550*bis* Criminal Code	Unauthorised access and maintenance of access to a computer system even with no intention to cause harm	Imprisonment between three months and one year (two years in case of intent) and/or a fine up to EUR 125,000
		Intentional abuse of access rights by an authorised user of a computer system	Imprisonment between 6 months and 2 years and/or a fine up to EUR 125,000
Spam	Article 14 Law of 11 March 2003	The use of electronic mail for advertising purposes without the prior, free, specific and informed consent of the addressee of the messages is forbidden.	Fine up to EUR 125,000

3.2 Law enforcement bodies

3.2.1 Police (www.police.be)

Belgian police consists of the federal police and 196 local police units engaged in community policing. The Belgian Federal Computer Crime Unit (FCCU) is part of the federal police, General Direction of Judicial Police, Direction of Financial and

Economic Crime. The FCCU works closely together with 17 regional Computer Crime Units spread over the country, which assist the local and federal police during cyber crime related investigations. The FCCU gives technical and logistics support to the local Computer Crime Units but has no hierarchical command over them. Where possible, the FCCU also works together with other judicial services, the government and the private sector to give advice and promote preventive action.

3.2.2 Courts (www.cass.be)

The court most likely to deal with computer crime is the Court of First Instance, criminal section (*Correctionele rechtbank/Tribunal correctionnel*). Against its decisions, appeal can be lodged with the Court of Appeal (*Hof van beroep/Cour d'appel*). The Supreme Court (*Hof van Cassatie/Cour de Cassation*) only hears points of law. Proceedings on the merits of the case are always preceded by an inquiry under the supervision of the investigating magistrate.

3.3 Reporting

3.3.1 Competent authorities

The FCCU should be alerted in all cases of computer crime, such as denial of service attacks, hacking, fraud and any major computer crime incidents. Smaller computer crime that has no impact on the safety of citizens or where the financial impact is low will be given a lesser degree of priority and should be dealt with by the local and federal police as part of their general duties.

3.3.2 Contact details

Federal Computer Crime Unit
Notelaarstraat 211 rue du Noyer
B – 1000 Brussel / Bruxelles
T : +32 2 743 74 74
F : +32 2 743 74 19
E: contact@fccu.be
URL: www.fedpol
Languages: French, Dutch, German, English

National Privacy Protection Commission
(*Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée*)
Hoogstraat 139 rue Haute
B – 1000 Brussel / Bruxelles
T: +32 2 213 85 40
F: +32 2 213 85 65
E: commission@privacy.fgov.be
URL: www.privacy.fgov.be
Languages: French, Dutch, German, English

3.3.3 Other reporting mechanisms

The most important initiative for securing information systems and networks is the computer virus alert point set up by the Belgian telecommunications regulator (www.bipt.be or www.ibpt.be). The purpose of this e-security platform is to react

quickly and accurately in case of virus attacks. Internet users can subscribe to a free mailing list to receive latest information on circulating computer viruses. The same service is available by SMS against payment of a small fee.

There are also several alert mechanisms for content related crimes.

Illicit content – Child pornography, racism and the promotion of games of chance are examples of explicitly forbidden Internet content in Belgium.

Harmful content – With regard to content that can generally be harmful to Internet users, in particular children, no specific legislation exists so far. However, a bill is under discussion and in the past years several soft law initiatives were taken in this respect.

- A special alert mechanism for illicit information on Internet exists on the website of the FCCU. Internet users and ISP's can notify any supposed illicit information on Internet via an e-mail (contact@gpj.be) or fill in a form directly on the website. A specific and more detailed form is available for child pornography. Notifications can be done on an anonymous basis and should contain as much useful information as possible, such as the URL of the website or the full heading of a news item.
- Another alert mechanism for child pornography has been set up by Child Focus. Useful information on this issue is posted on a specific website (www.childfocus-net-alert.be) with the purpose of increasing the sense for responsibility of Internet users. Anyone confronted with Internet content that can be harmful for children's integrity, can notify such content on an anonymous basis on the website or by calling a 24/7 accessible toll-free emergency number 110 (+32 2 475 44 99 from abroad). Child Focus itself does not carry out any investigation but works together with the police and judicial authorities on the basis of a protocol.
- Most ISP's in Belgium are member of the professional ISP federation ISPA. A co-operation protocol dated 28 May 1999 exists between ISPA and the Ministry of Justice. The purpose of the protocol is to combat illicit public content on Internet. It does not grant any right to ISP's to actively search for illicit content or to look into the content of private communication via Internet. Internet users can notify their ISP, send an e-mail (contact@gpj.be) to the FCCU (see above) or fill in the relevant for on the website (www.gpj.be) if they believe being confronted with illicit content. ISP's engage to notify the authorities through the same procedures as soon as they are aware of any supposedly illicit content.

3.4 Forensics

Evidence in Belgian criminal procedure is not regulated. All kinds of evidence may be submitted. Electronic evidence is admitted as a common form of evidence. The more authentic the evidence, the easier it will be to convince a judge during proceedings.

When confronted with computer crime (through a complaint or discovery by the police), the FCCU will carry out the initial inquiry and forensics under the supervision of the public prosecutor. Upon receipt of the report from the FCCU, the latter may order additional inquiry measures or pass the investigation on to an examining magistrate (*onderzoeksrechter/juge d'instruction*). For certain investigation measures such as searches, the examining magistrate has exclusive competence. In some cases, a prosecutor or judge will use a civil expert to carry out the investigation. The suspect may also rely on an expert in case of a counter argument.

The following specific computer crime investigation measures are available:

3.4.1 Data seizure

The prosecutor may decide to make a copy of the hard disk to put it on a hard disk at the forensic workstation. If necessary, (part of) the access to the data and the copies thereof may be blocked or the data may even be deleted, e.g. because it is impossible to make a copy or in case of viruses. The prosecutor must inform the system administrator of the data that were copied, blocked or deleted and must guarantee the integrity and confidentiality of the seized data, e.g. through encryption and digital signature. Seized data are admissible as documentary evidence and supporting evidence. In the case of documentary evidence, they are backed up by other material evidence and declarations of the suspects and witnesses.

3.4.2 Network searching

The investigating magistrate may order a search of the network if deemed necessary to reveal the truth. There must be a risk that the data would otherwise get lost and the search may not go beyond the computer system or parts thereof to which the persons authorised to use the searched system have access. Data located on a computer system abroad may be copied but not blocked and the investigating magistrate must inform the ministry of justice who will notify the country in question.

3.4.3 Involvement of experts

The investigating magistrate may order persons who have the necessary expertise to provide information on the working of the relevant informatics system or on how to get access to the relevant electronic data. The network administrator may for instance be asked to provide a password or to provide information on the security technique adopted for the system. If necessary to reveal the truth, e.g. because the system is too complex or because not enough qualified police staff is available, the investigating magistrate may order any relevant person but the suspect or his close relatives to carry out, if possible, certain operations on the system such as making the system work or searching for electronic data. Anyone aware of these investigation measures, including the person requested to co-operate, is bound by a duty of confidentiality. Refusal to

co-operate as well as breach of the confidentiality duty is subject to criminal sanctions. The Belgian State is liable for damage to the computer system or to the data as a result of these investigating measures.

3.5 References (www.just.fgov.be)

- Criminal Code (1867) and Code of Criminal Procedure [1808]
- Law of 28 November 2000 concerning informatics crime (*Wet inzake informaticacriminaliteit/Loi relative à la criminalité informatique*)
- Law of 8 December 1992 on privacy protection in relation to the processing of personal data (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard de traitement de données à caractère personnel*)
- Law of 14 July 1991 concerning trade practices and consumer information and protection (*Wet betreffende de handelspraktijken en de voorlichting en bescherming van de consument/Loi sur les pratiques du commerce et sur l'information et la protection du consommateur*)
- Law of 11 March 2003 on certain legal aspects of the information society (*Wet betreffende bepaalde juridische aspecten van de informatiemaatschappij/Loi sur certains aspects juridiques de la société de l'information*)

CHAPTER 4 Country report - Cyprus

4.1 Cypriot legislation on computer crimes

Various pieces of legislation have been enacted to tackle information technology related offences. More specifically, a law was enacted in 2004 for the purpose of ratifying the Cyber crime Convention 2001. The types of offences dealt with concern illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and fraud.

Furthermore, the Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996 (*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων) Νόμος του 1996*) prohibits the unauthorized interception of any private communication, subject to certain exceptions.

The Law Regulating Electronic Communications and Postal Services of 2004 (the Electronic Communications Law) (*Ο περί Ρύθμισης Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, Ν. 112(Ι)/2004*) prohibits any person, other than users communicating between themselves from time to time, to listen into, tap, store, intercept and/or undertake any other form of surveillance of communications without the consent of the users concerned, except where this is provided for by Law and where there is an authorisation by the Court.

In addition, specific laws such as the Law for the Processing of Personal Data (the Data Protection Law) (*Ο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001, Ν. 138(Ι)/2001 έως 37(Ι)/2003*) penalise spam, unauthorised interference with a record of personal data, receiving knowledge of data, extracting, altering, harming, destroying, processing, transmitting, notifying, making data accessible to unauthorized persons and allowing such persons to receive knowledge of the data, or exploiting the data in any way.

With regards to investigations, this law confers the power to the Commissioner for the Protection of Personal Data (*Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*) to assign officers of his Office the duty to carry out administrative researches and checks of any data record. For this purpose, she has the right to access personal data and collect any kind of information, without being restricted by any form of confidentiality obligation, except that of legal privilege. However, the Commissioner does not have access to the identity details of her colleagues who are mentioned in records kept for the purposes of national security or for the investigation of particularly serious crimes. Finally, the Commissioner is afforded the power to examine in person records kept for purposes of national security.

Relevant Incidents	Applicable provision	Description	Sanction
Target fingerprinting	Section 26 of the Data Protection Act	The collection, filing and other processing of personal data by means of fingerprinting is unlawful unless it is collected and recorded only by authorities which are bound to keep relevant files by virtue of law, e.g. for the purpose of monitoring the access to areas where confidential files are kept or to access-restricted installations.	Fines up to CYP 5,000 (approx. EUR 8,700) and/or warning with a specific time limit to cease the violation and/or temporary or permanent withdrawal of permits and/or destruction of records or suspension of processing and destruction of data.
Malicious code	Section 4 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Illegal access: intentionally and without right gaining access to the whole or any part of a computer system by infringing security measures.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
	Section 6 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Data Interference: Intentionally and without right damaging, deleting, deteriorating, altering or suppressing computer data.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.

	Section 7 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	System Interference: intentionally and without right seriously hindering the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
	Section 8 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Intentional and without right production, sale, procurement for use, import, distribution or otherwise making available of (i) A device designed or adapted primarily for the purpose of committing any offence related to illegal access, illegal interception, data interference and/or system interference; (ii) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed so that it be used for the purpose of committing any offence related to illegal access, illegal interception, data interference, system interference.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.

	Section 10 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Intentional and without right, with fraudulent or dishonest intent, causing of damage to the property of another by inputting, altering, deleting or suppressing computer data or by causing any interference with the functioning of a computer system, and as a result procuring without right, an economic benefit for oneself or for another.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
Denial of service	Section 6 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Data Interference: Intentionally and without right damaging, deleting, deteriorating, altering or suppressing computer data.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
	Section 7 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	System Interference: intentionally and without right seriously hindering the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
Account compromise	Section 4 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Illegal access: intentionally and without right gaining access to the whole or any part of a computer system by infringing security measures.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
Intrusion attempt	Section 4 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Illegal access: intentionally and without right gaining access to the whole or any part of a computer system by infringing security measures.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.

	Section 14 of the Protection of Confidentiality of Private Communications (Interception of Conversations) Law of 1996, Law No. 92(I)/1996	(a) Tap or intercept or attempt to tap or intercept or cause or allow or authorise any other person to tap or intercept any private communication, intentionally. (b) Use, attempt to use, instigate or cause or authorise another person to use or to attempt to use any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine for the purpose of tapping or intercepting any private communication, on purpose. (c) Reveal or attempt to reveal to any another person the content of any private communication, intentionally, while being aware or having reason to believe that the information was received by bugging or interception of private communication. (d) Use or attempt to use, on purpose, the content of any private communication, when being aware or having reason to believe that the information was received by tapping or interception of a private communication.	Imprisonment for up to three years.

Unauthorised access to information	Section 4 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Illegal access: intentionally and without right gaining access to the whole or any part of a computer system by infringing security measures.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.

	Section 14 of the Protection of Confidentiality of Private Communications (Interception of Conversations) Law of 1996, Law No. 92(I)/1996	(a) Tap or intercept or attempt to tap or intercept or cause or allow or authorise any other person to tap or intercept any private communication, intentionally. (b) Use, attempt to use, instigate or cause or authorise another person to use or to attempt to use any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine for the purpose of tapping or intercepting any private communication, on purpose. (c) Reveal or attempt to reveal to any another person the content of any private communication, intentionally, while being aware or having reason to believe that the information was received by bugging or interception of private communication. (d) Use or attempt to use, on purpose, the content of any private communication, when being aware or having reason to believe that the information was received by tapping or interception of a private communication.	Imprisonment for up to three years.

Unauthorised access to transmissions	Section 5 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004)	Illegal Interception: intentionally intercepting without right by technical means, computer data that is not transmitted to the public from or within a computer system.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
	Section 14 of the Protection of Confidentiality of Private Communications (Interception of Conversations) Law of 1996, Law No. 92(I)/1996	Use, attempt to use, instigate or cause or authorise another person to use or to attempt to use any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine for the purpose of tapping or intercepting any private communication, on purpose.	Imprisonment for up to three years.
	Section 99 of the Electronic Communications Law	Listening into, tapping, storing, intercepting and/or undertaking any other form of surveillance of communications without the consent of the users concerned.	Imprisonment not exceeding six months or fine not exceeding CYP 1,000 (approx. EUR 1,740)or both.
Unauthorised modification of information	Section 6 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	Data Interference: Intentionally and without right damaging, deleting, deteriorating, altering or suppressing computer data.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.
Unauthorised access to communication systems	Section 7 of Law of 2004 Ratifying the Cybercrime Convention of 2001 (Law No. 22(III)/2004).	System Interference: intentionally and without right seriously hindering the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	Imprisonment for up to five years or fine of up to CYP 20,000 (approx. EUR 34,000) or both such penalties.

	Section 14 of the Protection of Confidentiality of Private Communications (Interception of Conversations) Law of 1996, Law No. 92(I)/1996	(e) Tap or intercept or attempt to tap or intercept or cause or allow or authorise any other person to tap or intercept any private communication, intentionally. (f) Use, attempt to use, instigate or cause or authorise another person to use or to attempt to use any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine for the purpose of tapping or intercepting any private communication, on purpose. (g) Reveal or attempt to reveal to any another person the content of any private communication, intentionally, while being aware or having reason to believe that the information was received by bugging or interception of private communication. (h) Use or attempt to use, on purpose, the content of any private communication, when being aware or having reason to believe that the information was received by tapping or interception of a private communication.	Imprisonment for up to three years.

Spam	Section 106 of the Electronic Communications Law	Use of automated calling systems without human intervention (automatic calling machines) or facsimile machines (fax) or electronic mail or SMS messages for the purposes of direct marketing without prior consent. Automated calls for the purposes of direct marketing by any other means than the aforementioned are prohibited without the consent of the subscribers concerned.	Imprisonment not exceeding six months or fine not exceeding CYP 1,000 (approx. EUR 1,740) or both.
	Section 15 of the Data Protection Law	Processing by anyone for the purpose of the promotion, sale of goods or the provision of services at a distance, without the data subject having notified his consent to the person responsible for processing in writing.	Fines up to CYP 5,000 (approx. EUR 8,700) and/or warning with a specific time limit to cease the violation and/or temporary or permanent withdrawal of permits and/or destruction of records or suspension of processing and destruction of data.
	Section 10 of the Law on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce and Associated Matters of 2004	Commercial communication by a service provider established in the territory of the Republic, by electronic mail, with a recipient who has not requested it, without the communication being identifiable clearly and unambiguously as such, as soon as the recipient receives it.	Fine up to CYP 5,000 (approx. EUR 8,700) which may be doubled in the event of second or further conviction.

4.2 Law enforcement bodies

4.2.1 Police (www.police.gov.cy)

The Department of Economic Crime of the Criminal Investigation Office of the Police (*Γραφείο Διερεύνησης Οικονομικού Εγκλήματος (ΓΔΟΕ) του Τμήματος Ανίχνευσης Εγκλημάτων της Αστυνομίας*) is in charge of computer crime investigations. It is composed of teams of select detectives that bear the responsibility for the investigations of particularly serious cases on a national basis. In addition, it undertakes the investigation of serious cases, in which the investigations are extended to more than one districts or even abroad. In addition, the department cooperates closely with the Divisional Crime Investigation Departments (*Επαρχιακά Τμήματα Ανίχνευσης Εγκλημάτων*), Crime Prevention Squads and other departments of the police, for the prevention and investigation of crime.

The Prosecution Office is the direct legal advisor for police detectives and investigators. It is the office they will address for instant advice on issues concerning criminal law, criminal procedure and evidence. It is the contact point between the police and the Law Office of the Republic (Attorney General) (*Γραφείο του Γενικού Εισαγγελέα*). Almost all serious criminal case files are forwarded to the Prosecution Office where experienced criminal lawyers scrutinize them. Many are forwarded to the Law Office with comments and proposals or for consultancy. The rest are returned to the Divisional Police Headquarters with instructions for further investigation, prosecution or final classification. Members of the Prosecution Office undertake the drafting of proposed legislation related to the Police and participate in committees where such bills are discussed. Finally, the Criminalistic Services (*Υπηρεσία Εγκληματολογικών Ερευνών*, CSCP), situated at the Police Headquarters, is the main provider of forensic science support to the criminal justice system of the Cyprus Republic.

4.2.2 Courts

The courts exercising criminal jurisdiction most likely to deal with computer crime is the District Court of criminal jurisdiction (Επαρχιακό Δικαστήριο Ποινικής Δικαιοδοσίας) and the Supreme Court of Justice (Ανώτατο Δικαστήριο) in its appellate jurisdiction. Criminal proceedings are commenced by a charge preferred at the competent District Court. Every District Judge has jurisdiction to try all offences committed within the district in which the court is established and all offences committed within the Sovereign Base Areas by a Cypriot against a Cypriot.

4.3 Reporting

4.3.1 Competent authorities

The Criminal Investigation Office should be alerted in cases of major computer crime incidents, although police experience and willingness to deal with these issues is relatively limited. This is especially so for smaller scale and domestic computer crime incidents reported by private citizens and which involve unauthorised access to transmissions, unauthorised access to information, intrusion attempts and computer fingerprinting. The police are unlikely to give any particular degree of priority in investigating such crimes due to the inadequacy of awareness in such specialised issues.

The Commissioner for the Protection of Personal Data, which is the principal regulatory body dealing with offences such as spam and other unauthorized access to personal information, has the responsibility of ensuring the application of the Data Protection legislation. The Commissioner has a number of powers, inter alia reporting violations of the Law to the competent authorities and the Police in particular, imposing administrative sanctions, assigning to officers of her Office the duty to carry out administrative searches and making administrative checks of any data record, whether of her own accord or following a report. For this purpose, she has the right to access personal data and collect any kind of information, without being restricted by any form of confidentiality obligation, except that of legal privilege. The Commissioner also has the competence to investigate complaints relevant to the application of the law and the protection of the rights of the applicants when these concern the processing of personal data related to them. She also investigates applications seeking to monitor and ascertain the legality of processing and informs the applicants of her actions.

Finally, the Commissioner of Electronic Communications is conferred power to deal with issues concerning interference with communications networks as well as spam.

4.3.2 **Contact details**

Economic Crime Section – Criminal Investigation Office
Cyprus Police
pressoffice@police.gov.cy
T: +357 22 808067
F: +357 22 808714

Office of the Commissioner of Electronic Communications and Postal Regulation
Helioupoleos 12
1101 Nicosia
T: +357 22 693000
F: +357 22 693070
E-mail: info@octpr.org.cy

Office of the Commissioner for Personal Data Protection
40, Themistokli Dervi str.
Natassa Court, 3rd floor
1066 Nicosia
P.O. Box 23378
1682 Nicosia
T: +357 22 818456
F: +357 22 304565
E-mail: commissioner@dataprotection.gov.cy

4.3.3 Other reporting mechanisms

Cyprus legislation, and in particular the Law Ratifying the Cybercrime Convention of 2001 (*Ο περί της Σύμβασης κατά του Εγκλήματος μέσω του (Κυρωτικός) Νόμος του 2004, N. 22(III)/2004.*), establishes certain criminal offences in accordance with Chapter II of the Cybercrime Convention in relation to confidentiality, integrity and availability of computer data and systems. In particular, it criminalises:

Computer-Related Forgery:

Section 9 of the Law makes it an offence for a person to, intentionally and without right, input, alter, delete or suppress computer data, resulting in inauthentic data with the intent that such data be considered or acted upon for legal purposes as if they were authentic. This is regardless of the fact that the data were directly readable and intelligible. Such an offence is punishable with imprisonment for up to five years or with a fine of up to CYP 20,000 (approx. EUR 34,000) or with both such penalties.

Illicit content:

Offences related to Child Pornography - Section 11 of the Law Ratifying the Cybercrime Convention makes it an offence for a person to intentionally and without right:

(i) Produce child pornography for the purpose of its distribution through a computer system;
(ii) Offer or make available child pornography through a computer system;
(iii) Distribute or transmit (emit) child pornography through a computer system;
(iv) Promote child pornography through a computer system for oneself or for another;

Possess child pornography in a computer system or on a computer-data storage medium.

Such an offence is punishable with imprisonment for up to ten years or with a fine of up to CYP 25,000 (approx. EUR 43,000) or with both such penalties.

The term 'child pornography' includes pornographic material that visually depicts a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct as well as realistic images representing a minor engaged in sexually explicit conduct. Sexually explicit conduct is interpreted as to include intercourse between minors or between a minor and a person of age of the same or different sex, sodomy, masturbation, sadistic or masochistic behaviour within the framework of a sexual act.

Attempts, Aiding and Abetting:–

Section 13 of the Law Ratifying the Cybercrime Convention provides that a person who intentionally and without right aids or abets the commission of any of the offences relevant to illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, offences related to infringements of copyright and related rights, commits an offence punishable with imprisonment for up to five years or with a fine of up to CYP 20,000 (approx. EUR 34,000) or with both such penalties.

Racist and Xenophobic Content:

The Law Ratifying the Additional Protocol to the Cybercrime Convention Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems establishes the following criminal offences punishable with imprisonment for up to five years or with a fine of up to CYP 20,000 (approx. EUR 34,000) or with both such penalties:

(a) Dissemination of Racist and Xenophobic Material through Computer Systems: intentionally and without right distributing or otherwise making available to the public racist and xenophobic material promoting or inciting racial discrimination, hatred or violence, through a computer system.
(b) Racist and Xenophobic Motivated Threats: intentionally and without right threatening a person through a computer system acting on the basis of racism or xenophobia.
(c) Racist and Xenophobic Motivated Insult: intentionally and without right publicly insulting, through a computer system, a person that is, as a result of the insult, found subject to hatred, contempt or ridicule.
(d) Denial, Gross Minimisation, Approval or Justification of Genocide or Crimes Against Humanity: through a computer system, intentionally and without right denying, grossly minimising, approving or justifying acts constituting genocide or crimes against humanity, acting on the basis of racism and xenophobia.
(e) Aiding and Abetting: intentionally and without aiding or abetting the commission of any of the aforementioned offences.

- *Specific Obligations Regarding Commercial Communications and Spamming:*

Part II of the Electronic Commerce Law, Sections 9 to 11, prescribes the manner bywhich commercial communications may be sent by information society service providers for the promotion of goods, services or the image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a profession. Where promotional offers are being sent, such as discounts, premiums and gifts, they must be clearly identifiable as such, the conditions which are to be met for someone to be able to benefit from the said offers must be easily accessible, and the terms must be presented clearly and unambiguously. Promotional competitions or games must also be clearly identifiable as such. The conditions for participation must be easily accessible and the terms must be presented clearly and unambiguously.

Failure to comply with the above provisions may lead to the imposition of a penalty up to CYP 5,000 (approx. EUR 8,700) which may be doubled in the event of second or further conviction

More particularly, with regards to unsolicited commercial communication (spamming), Section 10 of the Law provides that a commercial communication by a service provider established within the territory of the Republic, by electronic mail, to a recipient who has not requested it, must be identifiable clearly and unambiguously as such, as soon as it is received by the recipient. In the event of a violation of these provisions, a person will be liable to a penalty up to CYP 5,000 (approx. EUR 8,700) which may be doubled in the event of second or further conviction.

Service providers undertaking unsolicited commercial communications by electronic mail must also consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

According to Section 11 of the Law, the use of commercial communications which are part of, or constitute, an information society service provided by a member of a regulated profession is permitted subject to compliance with the professional rules regarding the independence, dignity and honour of the profession and professional secrecy and fairness towards clients and colleagues.

This Section also confers power to the Minister of Industry, Commerce and Tourism to encourage professional unions and bodies to establish codes of conduct at national and community level in order to determine the types of information that can be given within the framework of commercial communication.

As for reporting mechanisms relevant to spam, Section 4 of the Electronic Commerce Law appoints the Minister of Commerce, Industry and Tourism as the Competent Authority responsible for ensuring the effective application of the Electronic Commerce Law. For this purpose, the Minister is under the obligation to have available the necessary means of control and investigation and in particular the necessary technical equipment and competent staff for achieving the effective application of the Electronic Commerce Law.

The Minister is also granted the power and function to determine the contact points to which recipients and service providers may refer by electronic means in order to:

(a) Obtain general information on the applicable legislation on matters relevant to electronic commerce and, in particular, in relation to their contractual rights and obligations as well as on the existing complaint and redress mechanisms available in the event of disputes, including practical aspects involved in the use of such mechanisms;
(b) Obtain the details of authorities, organisations, associations and or other providers in the Republic to which they may refer for further information or practical assistance.

The Electronic Commerce Law imposes a duty on the Minister to investigate violations of the provisions of the Law, either when a complaint is submitted to him or on his own initiative. When carrying out an investigation, the Minister must follow the procedure prescribed by the Law for the purpose of finding whether the provisions of the Law have been violated. Following an investigation, if the Minister considers that there has been a violation and if he deems this to be expedient, he has the power to make an application to the competent Court for the issuing of an injunction, including an interim order, against any person who, in his judgement, is involved or is responsible for a violation of the Law.

When the Minister exercises the said powers, he must take into consideration all of the interests involved, including the public interest, as well as the promotion of contracts regulated by independent organizations, professional associations and unions and other bodies active in the field of Information Society services.

The Electronic Commerce Law also confers power to the Court before which any application is pending to issue a restraining order, including an interim order ordering:

(a) The immediate seizure and/or non repetition of the violation;
(b) The taking up of such corrective measures according to the Court's judgment, within a prescribed time limit, for the purpose of terminating the illegal situation that has been created by the violation under consideration;

(c) The publication in whole or in part of the relevant decision of the Court or the publication of a restorative notification for the purpose of eliminating any continuing effects of the violation under consideration; and/or
(d) Any other act or measure that it may deem necessary or reasonable under the circumstances of the particular case.

4.4 Forensics

4.4.1 Presentation of Documents

The Evidence Law (*Ο περί Απόδειξης Νόμος, Κεφ. 9*) and the principles established by it apply to any criminal procedure introduced against any person for the punishment thereof for any criminal offence committed in violation of any law, or administrative act, establishing criminal offences.

According to Section 34 of the Law, the competent Court has a discretionary power to admit statements contained in an original document or a copy of an original document, if the statement is admissible as evidence. A 'document' is defined as any object on which any information or representation of any kind is registered or imprinted. A 'copy,' in relation to a document, is defined as anything on which the said information or representation has been copied by use of any medium, either directly or indirectly.

This general definition of the term 'document' has been introduced in 2004 replacing a previous definition which used to take technological developments into account. The previous provision stated that a document included a disc, music tape, electronic disc registering visual representations of writing or any other medium registering visual representations capable of being reproduced either by using another device or without using such device.

Although the new definition does not expressly provide that a document produced electronically is capable of being accepted as evidence, it may be inferred that due to the wide definition of the term, it may include information or representations reproduced directly or indirectly by electronic mediums. As a result, it may also be inferred that the competent courts are accorded wide discretionary powers with respect to the admissibility of any type of documents, including electronically produced ones.

4.4.2 Presentation of Apparatus, Machines, Equipment – Physical Evidence

According to the evidence rules and jurisprudence applicable in Cyprus, an object that is the subject matter of the case or that is relevant to the case before the Court can be presented as evidence to the Court. However, if it is practically impossible to bring it to Court or its visual appearance is not sufficient to lead the Court to conclusions, further evidence may be allowed by persons who came in contact with it, concerning the working condition of the apparatus, its relation to the defendant and the manner in which it was used by the defendant. An expert witness can give such evidence.

4.4.3 Evidence of Tapes, Recordings, Videos, etc

Such material may be admissible evidence and may present a tone of voice or visual characteristic. The registration made by the tape must be precise, strong (not faint) and of good quality and there must be no change or interference. The same is true for video cameras (e.g. attached on buildings). There is no need for the persons who were responsible for the registration to give evidence themselves.

4.4.4 Hearsay Computer Evidence

Evidence from a computer may be admissible as hearsay evidence if evidence is given that the computer was functioning properly and its content has not been altered. Therefore, evidence registered by mechanical means without human interference may be admissible if there is evidence that the machine was functioning properly. Similar provisions apply for discs, tape recorder tapes, sound tapes, or other means such as films, negatives, video tapes and electronic discs for the imprinting of visual representations, where sounds or other elements which are not visual representations are imprinted in a way that they can be reproduced by same with or without the use of other apparatus.

4.4.5 Criminal Procedure

The applicable legislation regarding criminal procedure is the Criminal Procedure Code. This Code basically introduces the English Criminal Procedure Rules with minor modifications.

4.4.6 Arrest of a Person on Reasonable Suspicion of Having Committed an Offence

The Criminal Procedure Code confers the power to the competent Judge, when he is satisfied by written affidavit that there is a reasonable suspicion that a person has committed an offence, or when the arrest or the detention is deemed reasonably necessary for preventing the commission of an offence or the escape of the person after the commission thereof, to issue a warrant of arrest authorising the arrest of the said person.

4.4.7 Search of Premises without a Warrant

Section 25 of the Law confers power on police officers to search without a warrant a person or premises, under certain conditions specified in the said warrant. Concerning premises, a police officer can, inter alia conduct a search without a warrant if he had reason to believe that an offence will or is being committed or has recently been committed. The type of offence must be one punishable with imprisonment exceeding two years. Furthermore, a police officer may enter and search any premises without a warrant by virtue of any legislation in force allowing for this. For example, the Customs And Excise Duties Law (*Ο περί Τελωνειακών Δασμών και Φόρων Καταναλώσεως Νόμος*) permits such entry and search without a warrant.

4.4.8 Search of Premises with a Warrant (Anton Pillar Order)

A warrant for the search of premises may be issued if the Judge is satisfied that there are reasonable grounds to believe that an item will be found therein intended to be used for the purpose of committing an offence. Here, the purpose is preventive. If the Judge is satisfied as to the necessity of issuing a warrant, he may issue such a warrant and authorize the person named therein to search the specified place and to seize and carry the evidence before the Court. The warrant may also authorise the apprehension of the occupier of the premises who is in possession of the specified object.

4.4.9 Commencement of Criminal Proceedings

Criminal proceedings are commenced by a charge preferred before the competent District Court. The charge is divided in two parts, the statement of the offence and the particulars of the offence. It must be signed by or on behalf of the person preferring same. Such person may be a private citizen, who is aggrieved by an act or omission constituting an offence under the relevant Law. The State may also institute a public prosecution. This right to bring a public prosecution is vested in the Attorney General of the Republic.

4.5 References

- Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996, Law No. 92(I)/1996 (Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων) Νόμος του 1996).
- Law Regulating Electronic Communications and Postal services of 2004, Law No. 112(I)/2004 (Ο περί Ρύθμισης Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, Ν. 112(I)/2004).

- Law for the Processing of Personal Data (Protection of the Person) Law of 2001, Law No. 138(I)/2001 as amended by Law No. 37(I)/2003 (Ο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001, Ν. 138(I)/2001 έως 37(I)/2003)
- The Evidence Law, Cap. 9, Cap 9, as amended by Law No. 42/1978, Law No. 86/1986, Law No. 54(I)/1994, Law No. 94(I)/1994 and Law No. 32(I)/2004 (Ο περί Απόδειξης Νόμος, Κεφ. 9)
- Criminal Procedure Code, Cap. 155 as amended by Law No. 93/1972, Law No. 2/1975, Law No. 12/1974, Law No. 41/1978, Law No. 162/1989, Law No. 142/1991, Law No. 9/1992, Law No. 10(I)/1996, Law No. 89(I)/1997, Law No. 54(I)/1998, Law No. 96(I)/1998 and Law No. 14(I)/2001

CHAPTER 5 Country Report: Czech Republic

5.1 Czech legislation on computer crimes

The broad reform of the Czech Criminal Code in 1991 has reflected the development of technologies and computer and network related offences by introducing Section 257a (Damaging or Misusing Data Carrier Records). Most of the incidents described below fall under one of the provisions of this section; in certain instances, other provisions of the Criminal Code (No 140/1961 Coll.) become relevant, too. Please note that the Criminal Code recognizes only criminal acts committed by natural entities, not by legal entities.

There is also a specific law (No 480/2004 Coll.) dealing *inter alia* with spreading unsolicited commercial communication (spam), often referred to as the "anti-spam law". This law treats spam as an administrative tort, rather than as a crime. There are also separate acts on personal data protection that can be relevant when an incident deals with unauthorised access and abuse of personal data

Currently, a brand new set of rules is expected to be passed as an outcome of the long-prepared reform of criminal law, including a new Criminal Code and Code of Criminal Procedure. In the text that advanced to the second reading of the legislative process at the time of writing of this report, computer-related crimes and criminal proceedings are covered in much more detail than in the present body of rules.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another form of cyber-crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime (e.g. theft, acts of terrorism)
Malicious code	Section 257a Criminal Code	Getting unauthorized access to data storage and changing, altering or deleting the data or making a change in the computer system in order to cause harm.	Imprisonment of up to one year, of up to three years when the crime is committed in an organized group, or between one and five years when causing serious damage; a fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a specific activity, or forfeiture of a specific object
	Section 249 Criminal Code	Unauthorized use of other people's items	Imprisonment up to 3 years, a fine up to Kč 5,000,000 (approx. EUR 300,000), or prohibition of a specific activity
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunication facility	Imprisonment up to 6 years or a fine up to Kč 5,000,000 (approx. EUR 300,000)
Denial of service	Section 257a Criminal Code	Unauthorized use, destroying, damaging or rendering useless the data on a data carrier with a harmful intent	Imprisonment up to 5 years, a fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a specific activity, or forfeiture of a specific object
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunication facility	Imprisonment up to 6 years or a fine up to Kč 5,000,000 (approx. EUR 300,000)
Account compromise	Section 257a Criminal Code	Intentionally gaining access to a data carrier followed by the unauthorised use, alteration, deletion or modification of such data	Imprisonment up to 5 years, a fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a specific activity, or forfeiture of a specific object
	Section 249 Criminal Code	Unauthorized use of other people's items	Imprisonment up to 3 years, a fine up to Kč 5,000,000 (approx. EUR 300,000), or prohibition of a special activity
Intrusion attempt	Section 257a *juncto* Section 8 Criminal Code	Preparatory measures in view of gaining access to a data carrier and unauthorized use of such data	Imprisonment up to 5 years, a fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a special activity, or forfeiture of a specific thing

	Section 249 *juncto* Section 8 Criminal Code	Preparatory measures in view of unauthorized use of other people's items	Imprisonment up to 3 years, a fine up to Kč 5,000,000 (approx. EUR 300,000), or prohibition of a specific activity
Unauthorised access to information	Section 257a Criminal Code	Gaining access to a data carrier and unauthorized use with the intention to cause harm, destroying, damaging or rendering useless of such data	Imprisonment of up to one year, of up to three years when the crime is committed in an organized group, or between one and five years when causing serious damage; a fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a specific activity, or forfeiture of a specific object
	Article 239 Criminal Code	Interception of private communication or data communication done by the communication provider.	Imprisonment of up to one year or prohibition of service provision.
		Interception of private communication or data communication.	Imprisonment of up to six months.
Unauthorised access to transmissions	Section 257a Criminal Code	Gaining access to a data carrier and unauthorized use of such data	Imprisonment of up to one year, of up to three years when the crime is committed in an organized group, or between one and five years when causing serious damage; a fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a specific activity, or forfeiture of a specific object
	Section 239 Criminal Code	Infringement of the confidentiality of messages transmitted by telephone, telegraph or similar public facility	Imprisonment up to 1 year or prohibition of a specific activity
	Section 240 Criminal Code	Disclosure of the contents of a confidential message or abuse of such message	Imprisonment up to 2 years or prohibition of a specific activity
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunication facility	Imprisonment up to 6 years or a fine up to Kč 5,000,000 (approx. EUR 300,000)
Unauthorised modification of information	Section 257a Criminal Code	Gaining access to a data carrier and unauthorized use, destroying, damaging or rendering useless	Imprisonment of up to one year, of up to three years when the crime is committed in an organized group, or between one and five years when causing serious damage; a

		of such data	fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a specific activity, or forfeiture of a specific object
Unauthorised access to communication systems	Section 257a Criminal Code	Gaining access to a data carrier and unauthorized use, destroying, damaging or rendering useless of such data, or interference with the hardware or software of a particular computer	Imprisonment of up to one year, of up to three years when the crime is committed in an organized group, or between one and five years when causing serious damage; a fine up to Kč 5,000,000 (approx. EUR 300,000), prohibition of a specific activity, or forfeiture of a specific object
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunication facility	Imprisonment up to 6 years or a fine up to Kč 5,000,000 (approx. EUR 300,000)
Spam	Section 11(1) Certain Information Society Services Act	Using electronic mail to send commercial communication without the prior consent of the recipient	Fine up to Kč 10,000,000 (approx. EUR 600,000)
	Section 178 Criminal Code	Unauthorized processing of personal data, even by negligence	Imprisonment up to 5 years, a fine up to Kč 5,000,000 (approx. EUR 300,000), or prohibition of a specific activity

5.2 Law enforcement bodies

5.2.1 Police (www.mvcr.cz/2003/policie.html)

Apart from the Foreigner police section and the Frontier police section, there are 14 regional police directorates and a national police presidium. The Criminal Police and Investigation Service (*Úřad služby kriminální policie a vyšetřování* - CPIS) co-ordinates the activities of the main specialized departments on the national level. The Department of Computer Crime (*Oddělení informační kriminality* - DCC) is the one responsible for monitoring and investigation of criminal activities relative to information technology. Its tasks include securing evidence on the Internet, service activities, and support to other departments within the CPIS.

5.2.2 Courts (www.nsoud.cz/en/index.html and www.justice.cz)

The court most likely to deal with computer crime is the District Court, criminal section (*Okresní soud, trestní senát*). In more serious cases where the relevant crime is

punished with a minimum imprisonment of 5 years the Regional Court, criminal section (*Krajský soud, trestní senát*) is competent as a court of first instance.

Against the decisions of the District Court, appeal can be lodged with the Regional Court (*Krajský soud*), while the Upper Court (*Vrchní soud*) will rule on any appeal against a decision of the Regional Court acting as a court of first instance.

The Supreme Court (*Nejvyšší soud*) decides in extraordinary legal remedies against appellate court decisions. It also evaluates final enforceable decisions of the courts and on their basis and in the interest of the uniformity of courts' decision-making adopts standpoints on the courts' decision-making in particular matters.

5.2.3 Office for Personal Data Protection (www.uoou.cz)

The Office for Personal Data Protection (*Úřad pro ochranu osobních údajů*) is the responsible organ in administrative proceedings against the perpetrators of administrative offences related to breaches of personal data protection and of unsolicited communication regulation. It collects and evaluates notifications on spam dissemination. It has limited rights to investigate such notifications and to issue an administrative fine of up to 33.000 EUR for breaking the Law on Information Society Services.

Any fines imposed for these offences are decided upon by the Office following the regulations in the Code of Administrative Procedure.

5.3 Reporting

5.3.1 Competent authorities

The DCC should be alerted in all cases of computer crime, such as denial of service attacks, hacking, fraud and any major computer crime incidents including software piracy and illegal content offences.

The Office for Personal Data Protection, established in 2000, is an independent agency, which supervises the observance of legally mandated responsibilities in the processing of personal data, maintains a register of instances of permitted personal data processing, deals with notifications and grievances from citizens concerning infringements of the law, and provides consultations in the area of personal data protection. It has also set up an alert point for the notification of spam, which can be accessed from its website (www.uoou.cz/spam.php3).

5.3.2 Contact details

Department of Computer Crime
(Oddělení informační kriminality)
Criminal Police and Investigation Service (Úřad služby kriminální policie a vyšetřování)
Police Presidium (Policejní prezidium - Policie ČR)
Strojnická 27
170 89 Praha 7
T : +420974 824 400
F : +420974 824 001
E: posta@mvcr.cz
URL: www.mvcr.cz
Languages: Czech, English

Office for Personal Data Protection (Úřad pro ochranu osobních údajů)
Pplk. Sochora 27
170 00 Praha 7
T : +420 234 665 501
F : +420 234 665 444
E : info@uoou.cz
URL: www.uoou.cz
Languages: Czech, English

5.3.3 Other reporting mechanisms

The Czech Republic, unlike many other European countries, has no special system, unit or mechanisms for collecting reports on computer crimes. The Office for Personal Data Protection collects reports on spam dissemination. The Police of the Czech Republic collects the information on other computer crime suspicions, including information about child pornography, racism or terrorist behavior. Such information is collected through standard channels, email and telephone desk, paper forms or through interchange of information between state bodies.

Consequently, content related crimes should be reported to the Department of Computer Crime or one of the local police units.

Illicit content – Child pornography and incitement to racial hatred are examples of explicitly forbidden Internet content in the Czech Republic.

Harmful content – With regard to content that can generally be harmful to Internet users, in particular children, no specific legislation exists so far.

Several related alert mechanisms exist in the Czech Republic.

- Internet users can report suspected child pornography on the Internet via the so-called Pink Line (*Růžová linka*), a telephone helpline (+420272 736 263; from 8 a.m. to 8 p.m. on working days and from 2 p.m. to 8 p.m. during weekends), set up primarily for children and young people with psychological problems.
- The Business Software Alliance offers a telephone hotline (224 811 748) and an online alert mechanism (www.bsa.cz/formular.asp) for the reporting of illegal software.
- Two projects have been started under the Safer Internet Plus programme (http://europa.eu.int/information_society/activities/sip/index_en.htm) in the Czech Republic. The first is called CzeSI and is focused on prevention through raising user awareness. The main goal is to teach users to recognize malicious content. The tools to be applied include media campaigns and international best practices.

- The second project is the Czech participation in the SAFT program. It is focused on child pornography and pornography, in particular on raising the knowledge of parents about this issue. Thus, it is also a prevention programme.

5.4 Forensics

Evidence in the criminal proceedings is regulated by the Code of Criminal Procedure. All kinds of evidence may be submitted except for evidence gathered by threat or use of unlawful coercion. The more authentic the evidence, the easier it will be to convince a judge during proceedings. Electronic documents have become a common evidence type in recent judicial practice.

The role of the police organs in general is to examine criminal complaints and investigate criminal acts. The police organs act independently and on their own initiative, however they may require the state attorney's (*státní zástupce*) permission for certain measures, especially when these interfere with civil rights.

With respect to computer crimes, the investigating organ might use a civil expert to assist in the investigation.

There are no specific computer crime investigation measures defined in the Code of Criminal Procedure. However, a number of provisions may be applied by analogy.

The following investigation measures are available:

5.4.1 Obligation to yield an object

Anyone who is in possession of an object relevant for the purposes of the criminal proceedings, is under the obligation to yield that object upon request by either a police organ, a state attorney, or a court. If the person in possession of such an object fails to comply with the request, the object may be seized by one of the abovementioned organs. The possessor of the object must receive a written confirmation of the seizure.

If the seizure involves processing personal data, the seizing organ is obliged to respect the right to protection of private and personal life of the data subject.

5.4.2 Interception and recording of telecommunication traffic

When there is a reasonable presumption that the means of telecommunication are or will be used to communicate information relevant for criminal proceedings, the court may order the interception and recording of telecommunications traffic for a maximum period of six months. This period may be prolonged by the court upon request of a police organ or state attorney. The telecommunications operator is under an obligation to cooperate with the investigating organ free of charge. If the

suspected activity is not established in the proceedings, the recordings must be destroyed.

5.4.3 Involvement of experts

According to the Code of Criminal Procedure, the investigating organ may order an expert opinion or involvement of experts whenever expert knowledge is necessary in the course of criminal proceedings. The specific rules on appointment of experts, right to refuse to provide an expert opinion and experts' remuneration can be found in a special law (Act on Certified Experts, Translators and Interpreters, *Zákon o znalcích a tlumočnících*, Law No. 36/1967 Coll.).

5.5 References (www.sbirka.cz)

- Criminal Code (*Trestní zákon*, Law No. 140/1961 Coll.)
- Code of Criminal Procedure (*Trestní řád*, Law No. 141/1961 Coll.)
- Act on Certified Experts, Translators and Interpreters (*Zákon o znalcích a tlumočnících*, Law No. 36/1967 Coll.)
- Code of Administrative Procedure (*Správní řád*, Law No. 71/1967 Coll.)
- Personal Data Protection Act (*Zákon o ochraně osobních údajů*, Law No. 101/2000 Coll.)
- Certain Information Society Services Act (*Zákon o některých službách informační společnosti*, Law No. 480/2004 Coll.)
- Electronic Communications Act (*Zákon o elektronických komunikacích*, Law No. 127/2005 Coll.)

CHAPTER 6 Country report - Denmark

6.1 Danish legislation on computer crimes

There are no specific laws regarding cyber crime in Denmark. However, the Danish Criminal Code includes a number of provisions dealing with cyber crime. The most important ones are found in article 169a (fake electronic money), article 193 (major disturbance in the operation of public means of communication), article 263(2) (unlawfully accessing information or computer programs), article 263(a) and 301(a) (unlawful use, sale etc. of access codes to certain information systems), article 279(a) (modification or deletion of computer programs with the purpose of obtaining an unlawful profit) and article 301 (unlawful use, production etc. of information identifying payment means assigned to others and payment card numbers).

A number of these cyber crime provisions are the result of a revision of the Criminal Code of 2002 with the purpose of updating the Criminal Code to cope better with the new types of criminal activities. Furthermore a number of provisions of the Criminal Code not specifically regulating cyber crime also have relevance for this kind of crime as can be seen in the table below.

Relevant Incidents	pplicable rovision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another form of cyber-crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime

Malicious code	Article 193 Criminal Code	Unlawfully causing a major disturbance in the operation of public means of communication, including publicly used telegraph or telephone services and information systems or installations	Imprisonment of up to 6 years. If the act was grossly negligent rather than intentional, the punishment is decreased to 6 months of imprisonment or a fine[8]
	Article 291 Criminal Code	Destroying or removing objects belonging to others	Imprisonment of up to 1 year and 6 months. If the incident causes malicious damage of a significant, systematic or organised nature, the punishment is imprisonment of up to 6 years. If the act was grossly negligent rather than intentional, the sanction is decreased to 6 months of imprisonment or a fine
Denial of service	Article 193 Criminal Code	Unlawfully causing a major disturbance in the operation of public means of communication, including publicly used telegraph or telephone services and information systems or installations	Imprisonment of up to 6 years. If the act was grossly negligent rather than intentional, the punishment is decreased to 6 months of imprisonment or a fine
	Article 263(2) Criminal Code	Unlawfully obtaining access to another person's information or programs designed to be used in an information system	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment.
Account compromise	Article 169(a) Criminal Code	Unlawfully producing, obtaining or distributing fake electronic money with the purpose of using it as authentic	Imprisonment of up to 1 year and 6 months; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment

[8] No size of fines is stated in the Criminal Code. As there are a limited number of IT-crime cases decided by the courts it is very difficult to give a reliable estimate of the size of fines under the relevant clauses of the criminal code.

	Article 263(2) Criminal Code	Unlawfully obtaining access to another person's information or programs designed to be used in an information system	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment.
Intrusion attempt	Article 263(2) Criminal Code	Unlawfully obtaining access to another person's information or programs designed to be used in an information system (preparatory measures in view of unauthorised access)	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment.
	Article 293(2) Criminal Code	Unlawfully hindering another person in disposing over an object	Imprisonment of up to 1 year or a fine. If the incident causes malicious damage of a significant, systematic or organised nature, or if other certain qualified circumstances apply, the penalty is increased to up to 2 years of imprisonment.
Unauthorised access to information	Article 263(a) Criminal Code	Unlawfully selling or distributing to a broad number of people a code or other means of access to a non-public information system to which the access is protected by code or other specific access requirements	Imprisonment of up to 1 year and 6 months or a fine. Under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
		Unlawfully passing on of a significant number of codes or other means of access to a non-public information system to which the access is protected by code or other specific access requirements	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment

		Unlawfully procuring or passing on a code or other mean of access as described in Article 263(a)(1) to a vital public information system or an information system used to process sensitive personal information or personal information on several individuals under Article 7(1) or 8(1) in the Data Protection Act	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
	Article 263(1) Criminal Code	Unlawfully (1) depriving someone of a sealed communication, or opening such a communication, or acquainting himself with its content, (2) obtaining access to places where other persons keep personal property, (3) secretly listening to or recording statements made private communications to which he has unlawfully obtained access with the aid of equipment	Imprisonment of up to 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
	Article 263(2) Criminal Code	Unlawfully obtaining access to another person's information or programs designed to be used in an information system (preparatory measures in view of unauthorised access)	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment.

	Article 301 Criminal Code	Producing, procuring, possessing or passing on (1) information identifying a mean of payment assigned to others, or (2) generated payment card numbers with the purpose to unlawfully use this information	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years imprisonment
	Article 301(a) Criminal Code	Unlawfully obtaining or passing on codes or other means of access to information systems to which the access is reserved to paying users where the access is protected by code or other specific access requirements	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
Unauthorised access to transmissions	Article 263(1) Criminal Code	Unlawfully (1) depriving someone of a sealed communication, or opening such a communication, or acquainting himself with its content, (2) obtaining access to places where other persons keep personal property, (3) secretly listening to or recording statements made private communications to which he has unlawfully obtained access with the aid of equipment	Imprisonment of up to 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment

	Article 263(2) Criminal Code	Unlawfully obtaining access to another person's information or programs designed to be used in an information system	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment.
Unauthorised modification of information	Article 171 Criminal Code	Using a fake document intended for use as evidence with the purpose of causing losses; this includes electronic documents	Imprisonment of up to 2 years or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
	Article 175 Criminal Code	Using fake declarations, where such declarations are mandatory under the law; this includes declarations on any readable medium	Imprisonment of up to 3 years or a fine
	Article 263(2) Criminal Code	Unlawfully obtaining access to another person's information or programs designed to be used in an information system	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment.
	Article 279(a) Criminal Code	Modifying or deleting information or programs for electronic data processing with the purpose of unlawfully obtaining a profit, or in any other way unlawfully seeking to affect the result of such data processing	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 8 years of imprisonment
Unauthorised access to communication systems	Article 263(a) Criminal Code	Unlawfully selling or distributing to a broad number of people a code or other means of access to a non-public information system to which the access is protected by code or other specific access requirements	Imprisonment of up to 1 year and 6 months or a fine. Under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment

		Unlawfully passing on of a significant number of codes or other means of access to a non-public information system to which the access is protected by code or other specific access requirements	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
		Unlawfully procuring or passing on a code or other mean of access as described in Article 263(a)(1) to a vital public information system or an information system used to process sensitive personal information or personal information on several individuals under Article 7(1) or 8(1) in the Data Protection Act	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
	Article 263(2) Criminal Code	Unlawfully obtaining access to another person's information or programs designed to be used in an information system	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment.
	Article 301 Criminal Code	Producing, procuring, possessing or passing on (1) information identifying a mean of payment assigned to others, or (2) generated payment card numbers with the purpose to unlawfully use this information	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years imprisonment

	Article 301(a) Criminal Code	Unlawfully obtaining or passing on codes or other means of access to information systems to which the access is reserved to paying users where the access is protected by code or other specific access requirements	Imprisonment of up to 1 year and 6 months or a fine; under certain qualified circumstances the penalty can be increased to up to 6 years of imprisonment
Spam	Article 6a Marketing Act	Approaching anyone by means of electronic mail, an automated calling system or facsimile machine with a view to the sale of goods, labour and services unless the addressee has requested him to do so	The courts may prohibit any acts contrary to the Marketing Act; the acting party shall pay damages in accordance with general Danish principles Non-compliance of a court order or an order by the Ombudsman may be punished with imprisonment of up to 4 months or a fine

6.2 Law enforcement bodies

6.2.1 Police (www.politiet.dk)

Danish police consists of the federal police and 54 local police districts. The federal police includes a section specialized in computer crimes called the National High-Tech Crime Centre (*Rigspolitien, IT-sektionen*, NHTCC). The NHTCC includes approximately 50 people which consist of both trained investigators and computer experts. NHTCC gives technical support to the local police districts including obtaining of evidence but has no hierarchical command over the local police districts.

6.2.2 Courts (www.cass.be)

There are three levels of regular courts: district courts (*byret*), appeal courts (*landsret*) and the Supreme Court (*hojesteret*). The courts hear both civil and criminal cases. The Supreme Court only hears points of law.

6.3 Reporting

6.3.1 Competent authorities

Computer crime reports are to be filed with the local police district and not with the NHTCC. If the computer crime includes violation of data protection rights under the Data Protection Act such violation can be reported to the Danish Data Protection Agency.

6.3.2 Contact details

The National High-Tech Crime Centre
Absalonsgade 9
DK-1658 Copenhagen V
Denmark
It-kriminalitet@politi.dk

The Danish Data Protection Agency
Borgergade 28, 5.
DK-1300 Copenhagen K
Denmark
dt@datatilsynet.dk
www.datatilsynet.dk

6.3.3 Other reporting mechanisms

A number of reporting mechanisms exist for violations of some more specific provisions. Possession, spreading etc. of child pornography can be reported to the organisation Save the Children Denmark (www.redbarnet.dk). Spam can be reported to the Danish Consumer Ombudsman (www.forbrugerombudsmanden.dk).

6.4 Forensics

Danish law contains only very few provisions regarding evidence. All kinds of evidence may be submitted and the courts are free to assess the evidentiary value of the evidence in question. For these reasons electronic evidence can also be submitted, and such evidence is quite common in cases regarding cyber crime.

Under article 786(a)(1) in the Administration of Justice Act, the police may require that internet access providers or telephone operators retain electronic data, including traffic data, if such data is likely to have any evidential importance during the investigations. Non-compliance to such a requirement may be punished with a fine, as specified in article 786(a)(4) of the Administration of Justice Act.

Furthermore, under article 786(a)(3) of the Administration of Justice Act internet access providers or telephone operators shall without undue delay pass on traffic data on other access providers or telephone operators where the network or service of these actors has been used for electronic communication, if such data is likely to have any evidential importance during the investigations. Non-compliance with such a requirement may be punished with a fine, as specified in article 786(a)(4) of the Administration of Justice Act.

6.5 References (www.retsinfo.dk)

- Criminal Code, act no. 960/2004 (*Straffeloven)*
- Marketing Act, act no. 699/2000 (*Markedsforingsloven)*
- Data Protection Act, act no. 429/2000 (*Personoplysningsloven)*
- Act on Services in the Information Society including Certain Aspects of Electronic Commerce, act no. 227/2002 (*Lov om tjenester i informationssamfundet herunder visse aspekter af elektronisk handel)*

CHAPTER 7 Country report - Estonia

7.1 Estonian legislation on computer crimes

According to the World Economic Forum, Estonia is one of the most competitive countries today among the new EU Member States. The Estonian telecommunications sector is one of the most developed in Central and Eastern Europe. Attitudes favouring innovative thinking and entrepreneurship have helped Estonia in a short time to level up with developed countries in the use of ICT. These factors, combined with general economic growth and macroeconomic stability have created a favourable basis for further progress in this field. An important role in this progress has been played by the free market conditions, since the telecommunications sector has been completely liberalised in Estonia since January 2001, when the special monopoly rights of the Estonian Telephone Company ended.

But there is no rose without a thorn. The rapid progress towards the information society in Estonia has been accompanied with a tide in cyber-crime as well. As an example, the incidence of various Trojan attacks against banking institutes attempting to obtain unauthorised access to bank accounts has increased by leaps and bounds. Currently, the prevailing cyber-crime trends in Estonia are computer related fraud (phishing, carding; 48% of all cyber-crimes in 2004), unlawful use of computers, computer systems or computer networks (38% of all cyber-crimes in 2004), computer viruses, worms, trojans and other malicious software being used as the main tool for various criminal attacks, the growing threat of botnets, cross-border organised criminal groups and increased paedophile activity on the Internet. Therefore the fight against cyber-crime is a priority for the Estonian law enforcement bodies.

First of all, it became important to update the existing legal system to provide a working basis for the police and courts. Fortunately Estonia had already taken the lead

in this process[9] in 2000. From that date on, three important e-laws (the Personal Data Protection Act (*Isikuandmete kaitse seadus)*, the Information Society Services Act (*Infoühiskonna teenuse seadus*) and the Telecommunications Act (*Elektroonilise side seadus*)) have entered into force, fixing penalties for spam and regulating commercial communications on the Internet. The Information Society Services Act provides a legal framework for information society service providers and establishes the organisation of supervision and liability for violation of this Act. It serves as an appropriate means to combat illicit public content on the Internet fixing the requirements for authorised service and data communication. As to child pornography, Estonia has ratified the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* in 2004, which provides a basis to deal with child pornography in the Internet. In 2003, the Estonian Riigikogu (Parliament) ratified the Convention on Cyber Crime by the Council of Europe.

For criminal offences (including those specified below, the court may impose a pecuniary punishment of 30 to 500 "daily rates". The court calculates the daily rate of a pecuniary punishment on the basis of the average daily income of the convicted offender. The daily rate applied shall not be less than the minimum daily rate, which is set at fifty EEK (approx. EUR 3,20) (§ 44 (1, 2) Criminal Code).

[9] Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, December 2000, a report prepared by McConnell International (www.mcconnellinternational.com/services/cyber-crime.htm).

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Not explicitly defined as a criminal act	Punished as an initial phase of some other cyber-crime	Depending on the follow up of the act
Malicious code	§ 206 (1, 2) Criminal Code	Unlawful replacement, deletion, damaging or blocking of data or programs in a computer, if significant damage is thereby caused, or unlawful introduction of data or programs in a computer, if significant damage is thereby caused	Imprisonment of up to 1[10] year or a fine of up to 500 daily rates
		The same act, if committed with the intention to interfere with the functioning of a computer or telecommunications system	Imprisonment of up to 3 years or a fine of up to 500 daily rates
	§ 208 (1, 2) Criminal Code	Dissemination of computer viruses	Imprisonment of up to 1 year or a fine of up to 500 daily rates
		The same act in case of repeat offence or in a manner which causes significant damage	Imprisonment of up to 3 years or a fine of up to 500 daily rates
	§ 213 Criminal Code	A person who obtains property benefits through the unlawful introduction, replacement, deletion or blocking of computer programs or data or other unlawful interference with a data processing operation, thereby influencing the result of the data processing operation	Imprisonment of up to 5 years or a fine of up to 500 daily rates

[10] For a criminal offence, the court may impose imprisonment for a term of thirty days to twenty years, or life imprisonment (§ 45 (1) Penal Code).

	§ 207 Criminal Code	Damaging or obstructing a connection to a computer network or computer system	A fine of up to 500 daily rates
Denial of service	§ 208 (1, 2) Criminal Code	Spreading of a computer virus	Imprisonment of up to 1 year or a fine of up to 500 daily rates
		The same act in case of repeat offence or in a manner which causes significant damage	Imprisonment of up to 3 years or a fine of up to 500 daily rates
	§ 213 Criminal Code	A person who obtains property benefits through the unlawful introduction, replacement, deletion or blocking of computer programs or data or other unlawful interference with a data processing operation, thereby influencing the result of the data processing operation	Imprisonment of up to 5 years or a fine of up to 500 daily rates
Account compromise	§ 217 (1) Criminal Code	Unlawful use of a computer, computer system or computer network by removing a code, password or other protective measure	A fine of up to 500 daily rates
Intrusion attempt	§ 217 (1, 2) Criminal Code	Unlawful use of a computer, computer system or computer network by removing a code, password or other protective measure	A fine of up to 500 daily rates
		The same act, if it causes significant damage, or is committed by using a state secret or a computer, computer system or computer network containing information intended for official use only	Imprisonment of up to 3 years or a fine of up to 500 daily rates

Unauthorised access to information	§ 217 (1, 2) Criminal Code	Unlawful use of a computer, computer system or computer network by removing a code, password or other protective measure	A fine of up to 500 daily rates
		The same act, if it causes significant damage, or is committed by using a state secret or a computer, computer system or computer network containing information intended for official use only	Imprisonment of up to 3 years or a fine of up to 500 daily rates
Unauthorised access to transmissions	§ 217 (1, 2) Criminal Code	Unlawful use of a computer, computer system or computer network by removing a code, password or other protective measure	A fine of up to 500 daily rates
		The same act, if it causes significant damage, or is committed by using a state secret or a computer, computer system or computer network containing information intended for official use only	Imprisonment of up to 3 years or a fine of up to 500 daily rates
Unauthorised modification of information	§ 206 (1) Criminal Code	Unlawful replacement, deletion, damaging or blocking of data or programs in a computer, if significant damage is thereby caused, or unlawful introduction of data or programs in a computer, if significant damage is thereby caused	Imprisonment of up to 1 year or a fine of up to 500 daily rates
	§ 208 (1, 2) Criminal Code	Spreading of a computer virus	Imprisonment of up to 1 year or a fine of up to 500 daily rates

		The same act in case of repeat offence or in a manner which causes significant damage	Imprisonment of up to 3 years or a fine of up to 500 daily rates
Unauthorised access to communication systems	§ 217 (1, 2) Criminal Code	Unlawful use of a computer, computer system or computer network by removing a code, password or other protective measure	A fine of up to 500 daily rates
		The same act, if it causes significant damage, or is committed by using a state secret or a computer, computer system or computer network containing information intended for official use only	Imprisonment of up to 3 years or a fine of up to 500 daily rates
Spam	§ 15[1] (1, 2) Information Society Services Act	The provision of information society services by a natural person which do not conform to the requirements provided for in this Act, regarding information that must be provided for commercial communications or transmission thereof	A fine of up to 300 fine units[11]
		The same act, if committed by a legal person	A fine of up to 50,000 EEK (3,195 EUR)

7.2 Law enforcement bodies

7.2.1 Police (www.pol.ee)

[11] For a misdemeanour, a court or an extra-judicial body may impose a fine of three up to three hundred fine units. A fine unit is the base amount of a fine and is equal to 60 EEK (ca 4 EUR) (§ 47 (1) Penal Code).

The Estonian Police is under the supervision of the Ministry of Internal Affairs, which supervises five central agencies – the Police Board (*Politseiamet*), the Security Police Board (*Kaitsepolitseiamet*), the Board of Border Guard (*Piirivalveamet*), the Citizenship and Migration Board (*Kodakondsus- ja migratsiooniamet*), and the Rescue Board (*Päästeamet*). It also administers the Inspection of Data Protection (*Andmekaitse Inspektsioon*) and Public Service Academy (*Sisekaitseakadeemia*) which is an educational institution providing applied higher education in the field of policing as well as in other administrative fields of the Ministry of Internal Affairs.

The central agency of the Estonian police system is the Estonian Police Board which manages, directs and co-ordinates the activities of all police units under its administration. The Police Board is also responsible for the development of new working methods, technological support and international cooperation. The Estonian Police has four national units: the Central Criminal Police (*Keskkriminaalpolitsei*), the Central Law Enforcement Police (*Julgestuspolitsei*), the Forensic Service Centre (*Kohtuekspertiisi ja Kriminalistika Keskus*) and the Police School (*Sisekaitseakadeemia Politseikolledž*). There are 4 territorial police units called Police Prefectures (*Politseiprefektuurid*).

The Central Criminal Police (CCP) co-ordinates the activities of the criminal police in the whole state and organises international cooperation. The CCP investigates crimes committed by criminal organisations, drug crimes, economical crimes and IT crimes exceeding the service areas of police prefectures, crimes related to money laundering and crimes requiring extensive international cooperation or central coordination because of their danger to society. For dealing with various information technology crimes there is an IT Crimes Unit (*Infotehnoloogiakuritegude talitus*) in the CCP.

Additionally, there is a Forensic Service Centre (FSC), whose main task is to conduct forensic examination (18 main areas including IT), participate in gathering evidence as an impartial specialist, keep relevant databases and data collections, provide professional training and equip police agencies with forensic equipment. The FSC IT forensic team provides computer forensic support for the whole of the Estonian police. An initiative has been launched to set up local IT crime units in police prefectures in order to also have a cyber-crime investigation capacity at local level. On top of that an EU twinning project is underway in Estonia which involves several cyber-crime experts from Interpol and other Member States of EU. This project is targeted to converting members of the Estonian police into an effective anti-cyber-crime organisation[12].

[12] Alar Must. Dealing with Cybercrime in a Post-Soviet Country – Estonia. *6th International Conference on Cyber Crime.* Cairo, Egypt, 13 – 15 April 2005 (www.interpol.org/Public/TechnologyCrime/default.asp).

7.2.2 Courts (www.kohus.ee)

Estonia has a three-level court system. County courts (*Maakohtud*), city courts (*Linnakohtud*) and administrative courts (*Halduskohtud*) adjudicate matters in first instance. The majority of courts of first instance are situated in county centres. Appeals against decisions of courts of first instance shall be heard by courts of second instance. The Courts of appeal (*Ringkonnakohtud*, sometimes also called circuit courts) function as courts of second instance, and are situated in Jõhvi, Tartu and Tallinn. The Supreme Court (*Riigikohus*), situated in Tartu, is the court of the highest instance. A statement of claim is filed with the court of first instance, an appeal with the court of second instance and an appeal in cassation with the court of third or the highest instance. A case can be heard in the Supreme Court only after all previous court instances have been passed. The filing of an appeal is governed by respective codes of court procedure.

7.3 Reporting

7.3.1 Competent authorities

In Estonia there is no way to contact CCP IT Crime Unit directly, either by phone or through another means of communication. All crimes, notwithstanding there specificity, can be reported through the free of charge short number 110 (within Estonia). The CCP IT Crime Unit deals with major cyber crimes, such as distributed denial of service and denial of service attacks, hacking, fraud and any other significant computer crime incident. Smaller computer crimes that do not pose any threat to the safety of citizens or where the financial interest is low will be given a lesser degree of priority and should be dealt with the local police prefectures as one of their common duties.

7.3.2 Contact details

Central Criminal Police
Tööstuse 52
11611 Tallinn
T: +372 612 3810; +372 612 3811
F: +372 612 3726
E: keskkriminaalpolitsei@kkp.pol.ee
E-mail(IT Crime Unit): itkt@kkp.pol.ee
URL: www.pol.ee
Languages: Estonian, Russian, English

Forensic Service Centre
Pärnu mnt 328
11611 Tallinn
T: +372 612 5300
F: +372 612 5309
E: kohtuekspertiis@kekk.pol.ee
URL: www.pol.ee
Languages: Estonian, Russian, English

7.3.3 Other reporting mechanisms

There are no other reporting mechanisms in Estonia save the ISPs who can give an advice in case of common problems. There is no centrally controlled virus alert point set up in Estonia; all relevant information about recent events in the virus world can only be retrieved from antivirus software providers. Illicit and harmful content are dealt with as common crimes without any special procedures or reporting mechanisms provided.

7.4 Forensics

Evidence in a criminal lawsuit is not regulated in Estonia. All forms of evidence are legally acceptable. Electronic evidence is equivalent with all others. As with all other offences, investigative bodies and prosecutor's offices conduct criminal proceedings upon the appearance of facts referring to an IT criminal offence.

The prevailing practice up until now has been that the hardware confiscated by the prosecutor is sent according to the expertise procedure to the FSC to be submitted to information technology expertise. The resulting expertise evidence would be added to the expertise dossier. On average, the FSC IT expertise would take up to 30 days depending on the amount of work the experts have at hand. Therefore, in case of the need for a prompt decision, it is important that the computer investigation can be carried out in the CCP and in local police prefectures as well.

A computer investigation is conducted on the basis of an order of a Prosecutor's Office, a court ruling, or an order of a preliminary investigation judge on the basis of a court ruling. In cases of urgency, an investigative body may conduct computer or computer network investigations on the basis of an order of the investigative body without the permission of a Prosecutor's Office, but in such case the Prosecutor's Office shall be notified of the investigation within twenty-hour hours and Prosecutor's Office shall decide on the admissibility of the search.

If a search is conducted, the search warrant shall be presented for examination to the person whose premises are to be searched or to his or her adult family member, or to a representative of the legal person or the state or local government agency whose premises are to be searched. He or she shall sign the warrant to that effect. In the absence of an appropriate person or representative, the representative of the local government shall be involved.

In the CCP IT Crime Unit the computer and computer network investigation has been a rather common daily job for the last couple of years, using the methodology worked out by FSC experts. If there is a need, IT specialists from other institutions may be involved. In practice, mainly IT specialists from central banks have been involved. The IT Crime Unit shall not refuse to order an expert assessment requested by the suspect if the facts for the ascertainment of which the assessment is requested may be essential for the adjudication of the criminal matter.

The following main specific computer crime investigation measures are available:

7.4.1 Data seizure

Depending on the circumstances, a copy of the hard disk can be made and loaded onto a hard disk at the workstation of the CCP IT Crime Unit having at their disposal a laboratory computer configuration. Alternatively, the computer can be taken to the prosecuting police office, so that the investigation operation can be performed there. The prosecutor is obliged to inform the computer system administrator about the data that have been copied, blocked or deleted and must guarantee the integrity and confidentiality of the seized data. Seized data are admissible as full right documentary or supporting evidence; when needed, it can be complemented by other material evidence together with statements of suspects and witnesses.

7.4.2 Network searching

The investigative body may order a search of a computer network during the investigation process if the relevant data would otherwise be not accessible. In case of major cyber crime incidents, the CCP IT Crime Unit would carry out the network search, since they have the required expertise in this field. But the search would not exceed the authorised limits. Data located on a computer system abroad can be copied, although this action can only be undertaken after the investigative body has informed the Ministry of Internal Affairs, in order to notify this action to its counterpart in the country involved.

7.4.3 Involvement of experts

Upon appointment of an expert, the body conducting the proceedings of a cyber-crime investigation shall give preference to a FSC expert or an officially certified expert. However, any other person with the relevant knowledge about the IT system under consideration or possessing the necessary skills to access the relevant electronic data may also be appointed as an expert. An expert is required to refuse to conduct the expert assessment if he or she is not impartial with regard to the criminal proceeding.

If an expert assessment is arranged outside FSC, the body conducting the proceedings shall ascertain whether the person to be appointed as an expert is sufficiently impartial and consents to conduct the expert assessment. If a person who has not been sworn in is appointed as an expert, he or she shall be warned about criminal punishment for rendering a knowingly false expert opinion. The body conducting a proceeding may request an expert assessment to be conducted in FSC and use an expert opinion rendered in a foreign state as evidence in the adjudication of a cyber criminal matter. An expert conducting an expert assessment has the right to refuse to conduct the expert assessment if the assessment materials submitted to him or her are not sufficient or if the expert assignments set out in the ruling on the expert assessment are outside his or her specific IT technology expertise. An expert is required to maintain the confidentiality of the facts which become known to him or her during the expert assessment. Cybercrime evidence shall be collected in a manner which is not harmful to the honour and dignity of the persons participating in the collection of the evidence and which does not cause unjustified damage.

7.4.4 Internet monitoring

Internet monitoring is not a regular procedure which is conducted on an every day basis in CCP IT Criminal Unit. It is carried out only in special cases when there is sufficient reason to believe that relevant evidence may be procured by it.

7.5 References (www.riigiteataja.ee)

- Penal Code (*Karistusseadustik*), passed 6 June 2001, entered into force 1 September 2002
- Code of Criminal Procedure (Kriminaalmenetluse seadustik), passed 12 February 2003, entered into force 1 July 2004.
- Databases Act (*Andmekogude seadus*), passed 12 March 1997, entered into force 19 April 1997.
- Public Information Act (*Avaliku teabe seadus*), passed 15 November 2000, entered into force 1 January 2001.
- Digital Services Act (*Digitaalallkirja seadus*), passed 8 March 2000, entered into force 5 December 2000.
- Personal Data Protection Act (*Isikuandmete kaitse seadus*), passed 12 February 2003, entered into force 1 October 2003.
- Information Society Services Act (*Infoühiskonna teenuse seadus*), passed 14 April 2004, entered into force 1 July 2004.
- Telecommunications Act (*Elektroonilise side seadus*), passed 8 December 2004, entered into force 1 January 2005.

CHAPTER 8 Country Report: Finland

8.1 Finnish legislation on computer crimes

Finland has enacted very few laws regarding computer crime, but applies and supplements the existing traditional provisions, like many other OECD countries. More specific computer crime related provisions are enacted only when needed, and the current Penal Code is quite comprehensive. The Finnish Penal Code contains the offences, which are sanctioned by imprisonment or fines. Some special laws (e.g. the Data Protection Act and the Act on the Protection of Privacy in Electronic Communications) also contain some offences, but these are typically only sanctioned with fines.

Relevant Incidents	Applicable provision	Description	Sanction
Target fingerprinting[13]	Article 38:8 Penal Code (Computer break-in)	(1) Using an authorized access code or otherwise unlawfully breaking the protection of an information system, or breaking into a separately protected part of such a system. An attempt is punishable.	Imprisonment of up to 1 year or a fine
		(2) Unlawfully obtaining information contained in a computer system without hacking, using a technical device. An attempt is punishable.	Imprisonment of up to 1 year or a fine
Malicious code[14]	Article 34:9a Penal Code (Criminal computer mischief)	(1) Producing or distributing a computer program or programming instructions designed to cause harm to automatic data processing or the functioning of a data system or telecommunications system, or to damage the data or software contained in such a system, with the intention to cause harm to automatic data processing or the functioning of a data system or telecommunications system,	Imprisonment for at most 2 years or a fine

[13] In *computer fingerprinting, account compromise* and *intrusion attempt* cases the boundary setting between computer break-in and unauthorised use is difficult and also overlapping to some extent. In both provisions the attempt is punishable, but for unauthorised use the perpetrator must actively use the system and not only break its protection. In order to qualify as unauthorised use, the system need not necessarily have been protected by security measures, and the sanction is also more severe than that of computer break-in.

[14] In certain situations deploying malicious code might also be punishable under article 35:2 (aggravated criminal damage), 36:1 (fraud), 36:2 (aggravated fraud), 38:5 (interference), or 38:6 (aggravated interference). Article 34:9a might also be applied to spyware when the provisions of the Personal Data Act are not abided by, or the Act on the Protection of Privacy in Electronic Communications, article 42:2 (2) can be applied.

		(2) Making available guidelines for the production of a computer program or set of programming instructions or distributing such guidelines, with the intention to cause harm to automatic data processing or the functioning of a data system or telecommunications system,	Imprisonment for at most 2 years or a fine
Denial of service[15]	Article 38:5 Penal Code (Interference)	Tampering with the operation of a device used in postal, telecommunications or radio traffic, by mischievously transmitting interfering messages over radio or telecommunications channels, or similarly unlawfully hindering or interfering with postal, telecommunications or radio traffic	Imprisonment for at most 2 years or a fine
Account compromise (see footnote 1)	Article 38:8 Penal Code (Computer break-in)	(1) Using an authorized access code or otherwise unlawfully breaking the protection of an information system, or breaking into a separately protected part of such a system. An attempt is punishable.	Imprisonment of up to 1 year or a fine
		(2) Unlawfully obtaining information contained in a computer system without hacking, using a technical device. An attempt is punishable.	Imprisonment of up to 1 year or a fine

[15] In certain situations this might also be covered by article 38:6 (Aggravated Interference) or 38:7 (Petty interference).

	Article 28:7 Penal Code (Unauthorised use)	Unlawfully using the movable property or the immovable machine or equipment of another person. An attempt is punishable.	Imprisonment up to 1 year or a fine
Intrusion attempt (see footnote 1)	Article 38:8 Penal Code (Computer break-in)	(1) Using an authorized access code or otherwise unlawfully breaking the protection of an information system, or breaking into a separately protected part of such a system. An attempt is punishable.	Imprisonment of up to 1 year or a fine
		(2) Unlawfully obtaining information contained in a computer system without hacking, using a technical device. An attempt is punishable.	Imprisonment of up to 1 year or a fine
	Article 28:7 Penal Code (Unauthorised use)	Unlawfully using the movable property or the immovable machine or equipment of another person. An attempt is punishable.	Imprisonment up to 1 year or a fine
Unauthorised access to information	Article 38:8 Penal Code (Computer break-in)	(1) Using an authorized access code or otherwise unlawfully breaking the protection of an information system, or breaking into a separately protected part of such a system. An attempt is punishable.	Imprisonment of up to 1 year or a fine
		(2) Unlawfully obtaining information contained in a computer system without hacking, using a technical device. An attempt is punishable.	Imprisonment of up to 1 year or a fine

	Article 28:7 Penal Code (Unauthorised use)	Unlawfully using the movable property or the immovable machine or equipment of another person. An attempt is punishable.	Imprisonment up to 1 year or a fine
	Article 38:3 Penal Code (Message interception)	1) Unlawfully opening a letter or another closed communication addressed to another, or hacking into the contents of an electronic or other technically recorded message which is protected from outsiders. An attempt is punishable.	Imprisonment up to 1 year or a fine
		2) Unlawfully obtaining information on the contents of a call, telegram, transmission of text, images or data, or another comparable telemessage or on the transmission or reception of such a message. An attempt is punishable.	Imprisonment up to 1 year or a fine
	Article 38:4 Penal Code (Aggravated message interception)	Using a position in the service of a telecommunications company or other special position of trust to intercept a message as described above. An attempt is punishable.	Imprisonment up to 3 years
		Using a computer program or special technical device designed or altered for such purpose, or another special method to intercept a message as described above. An attempt is punishable.	Imprisonment up to 1 year or a fine

		Intercepting a message as described above when the message has a particularly confidential content or when the act constitutes a serious privacy infringement, and the interception can be considered aggravated when assessed as a whole. An attempt is punishable.	Imprisonment up to 1 year or a fine
	Article 30:4 Penal Code (Business espionage)	Unlawfully obtaining information regarding the trade secret of another by entering an area closed to unauthorised persons or accessing an information system protected against unauthorised persons, by gaining possession of or copying a document or other record, or in another comparable manner, or by using a special technical device, with the intention of unlawfully revealing or using the trade secret. An attempt is punishable	Imprisonment up to two years or a fine
Unauthorised access to transmissions	Article 38:5 Penal Code (Interference)	Tampering with the operation of a device used in postal, telecommunications or radio traffic, by mischievously transmitting interfering messages over radio or telecommunications channels, or similarly unlawfully hindering or interfering with postal, telecommunications or radio traffic	Imprisonment for at most 2 years or a fine

	Article 38:6 Penal Code (Aggravated interference)	(1)Interfering with communications as described above, making use of a position in the service of an institution referred to in the Telecommunications Act, a cable operator referred to in the Cable Transmission Act (307/1987) or a public broadcasting organization or any other special position of trust	Imprisonment between four months and four years
		(2) Interfering with communications as described above, when the transmissions are made in order to protect human life and the interference is aggravated when assessed as a whole	Imprisonment between four months and four years
Unauthorised modification of information[16]	Article 35:1 Penal Code (Criminal damage)	Unlawfully and intentionally deleting, defacing, or concealing data recorded on an information device or other recording	Imprisonment up to 1 year or a fine
	Article 36:1 Penal Code (Fraud)	(1) Deceiving or taking advantage of an error of another to coerce this person to behaviour which will cause economic loss, in order to obtain an unlawful financial benefit for the perpetrator or another party, or in order to harm another. An attempt is punishable.	Imprisonment up to two years or a fine

[16] In certain situations this incident may be also punishable as article 30:4 (business espionage), or article 34:1 (criminal mischief).

		(2) Committing the crime referred to in (1), by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, in order to falsify the end result of data processing. An attempt is punishable.	Imprisonment up to two years or a fine
	Article 36:2 Penal Code (Aggravated fraud)	Committing fraud as described above, when the fraud 1) involves the seeking of considerable benefit, 2) causes considerable loss, 3) is committed by taking advantage of a position of a trust, or 4) is committed by taking advantage of a special weakness or other insecure position of another and the fraud is aggravated when assessed as a whole (2) An attempt is punishable	Imprisonment between four months and four years
Unauthorised access to communication systems	Article 28:7 Penal Code (Unauthorised use)	Unlawfully using the movable property or the immovable machine or equipment of another person. An attempt is punishable.	Imprisonment up to 1 year or a fine
	Article 38:8 Penal Code (Computer break-in)	(1) Using an authorized access code or otherwise unlawfully breaking the protection of an information system, or breaking into a separately protected part of such a system. An attempt is punishable.	Imprisonment of up to 1 year or a fine

		(2) Unlawfully obtaining information contained in a computer system without hacking, using a technical device. An attempt is punishable.	Imprisonment of up to 1 year or a fine
Spam	Article 42:2 (8) Act on the Protection of Privacy in Electronic Communications	The use of electronic mail for direct marketing purposes is forbidden when addressing 1) Natural persons who have not given their prior consent, and 2) Legal persons who have specifically prohibited it	A fine If the offence is deemed petty, no sentence shall be passed.

8.2 Law enforcement bodies

8.2.1 Police (www.poliisi.fi)

Finnish police have a three-tier organization. At the top is the Police Department of the Ministry of the Interior. Directly below it are the Provincial Police Commands (5), the national units, the police training establishments, the Police Technical Centre, and functionally also the Helsinki Police Department. The third level is the local police, who fall administratively under the State Local Districts. The District Police operate under their Provincial Police Command. The Åland Islands form their own independent police district.

One of the national units is the National Bureau of Investigation [*Keskusrikospoliisi*], which operates directly under the Police Department of the Ministry of the Interior. In 1998 a computer crime squad was established. This group is responsible for e.g. investigating computer crimes, educating the police force regarding computer-related offences, and helping the authorities in gathering and processing electronic evidence.

8.2.2 Courts (www.oikeus.fi)

The courts most likely to deal with computer crime are the District Courts (*Käräjäoikeus*). The decision of a District Court can normally be appealed in a Court of Appeal (*Hovioikeus*). Against these decisions, appeal can again be lodged with the Supreme Court (*Korkein Oikeus*), provided that the Supreme Court grants leave to do so. Prosecution is only possible after charges have been brought, and if there is a prima facie case against the suspect. The pre-trial investigation is a task for the police.

8.3 Reporting

8.3.1 Competent authorities

All cases of computer crime should be signalled to the local police. The Provincial Police Commands are in charge of cooperation between the local police and the National Bureau of Investigation within their province, and decide which duties are handled jointly and what the command structure should be in such cases. The National Bureau of Investigation also has a special e-mail contact point (vihje.internet@krp.poliisi.fi) for Internet related crimes. The Data Protection Ombudsman guides and controls the processing of personal data and provides related consultation.

8.3.2 Contact details

National Bureau of Investigation
(*Keskusrikospoliisi*)
Jokiniemenkuja 4
01370 Vantaa
Postal address : PL 285
01301 Vantaa
T : +358 9 8388 661
F : +358 9 8388 6536
E: krp-kirjaamo@krp.poliisi.fi
URL: www.keskusrikospoliisi.fi
Languages: Finnish, Swedish, English

Data Protection Ombudsman
(*Tietosuojavaltuutetun toimisto*)
Albertinkatu 25 A
Postal Address : PL 315
00181 Helsinki
T: +32 2 213 85 40
F: +32 2 213 85 65
E: tietosuoja@om.fi
URL: www.tietosuoja.fi
Languages: Finnish, Swedish, English

8.3.3 Other reporting mechanisms

The Finnish Communications Regulatory Authority (www.ficora.fi) has a group called CERT-FI (Computer Emergency Response Team FICORA), which focuses on information security incidents and their control. CERT-FI receives the notifications of telecommunications operators concerning information security incidents and threats. It also follows up on worldwide current events concerning information security incidents and responses to them. Warnings are published on the web site of Ficora, and they are also made available through email, RSS service (really simple syndication) or by SMS. Some of the warnings are also published in teletext.

There are no special penal provisions regarding the content of computer networks, but the traditional provisions of the Penal Code usually cover all kinds of communication. Thus, they can be applied to the publication or distribution of a message regardless of the technology or medium used, including the Internet and other computer networks.

Additionally, there are a number of regulatory organisations involved in mass media, whose decisions may apply on the Internet. The Council for Mass Media (http://www.jsn.fi, *Julkisen sanan neuvosto)* is a coregulatory organisation without any legislative or governmental mandate, whose decisions are published and commonly followed by any organisation that has subscribed to it.

The content of audiovisual programs is restricted by the legislation on Classification of Audiovisual programs. The Finnish Board of Film Classification (http://www.vet.fi,

Valtion elokuvatarkastamo) is the organisation responsible for compliance verification. The Board has also opened an information service regarding audiovisual programs and games age limits, meant especially for parents.

Illicit and harmful content[17] – public incitement to an offence, dissemination of depictions of violence, pictures violating sexual morality, child pornography, violation of religious freedom, ethnic agitation and warmongering are all examples of explicitly forbidden content in Finland. The provisions forbidding such content could also be applied on the Internet.

A special alert mechanism for reporting child pornography and violations of children's rights exists on the website of Pelastakaa Lapset- Rädda Barnen (http://www.pelastakaalapset.fi), where any supposed illicit and harmful information on the Internet can be signalled via e-mail (netti@pela.fi), via phone (+358 9 41355444), via postal service or by filling out an online form:

http://www.pelastakaalapset.fi/nettivihje/laheta-vihje.php

Notifications can be submitted on an anonymous basis. Nettivihje, the contact point of Pelastakaa Lapset, defends children's rights on the Internet, and provides relevant information through its website. It maintains a server to fight against illicit and harmful content, and cooperates closely with the international network Inhope. It also coordinates its activities with the National Bureau of Investigation, the competent authorities and Finnish service providers.

In 2001 the biggest operators in Finland have also published a special code of conduct, entitled "Netiquette" (*Netiketti*) to promote good conduct on the Internet[18].

8.4 Forensics (www.oikeus.fi)

Evidence in Finnish criminal procedure is not regulated, and electronic evidence is admitted as a common form of evidence.

The police will commence a pre-trial investigation if there is a reason to suspect that a crime has been committed. Not all reports of offences lead to pre-trial investigation. The general principles are laid down in the Pre-Trial Investigation Act. In the pre-trial investigation the police will establish whether or not an offence has actually been committed, under what circumstances it occurred and the identity of the parties concerned. The pre-trial investigation will also establish the extent of the injury or damage caused by an offence, the gain affected by the offender and the demands of the injured party. The police have a duty to conduct pre-trial investigation without undue delay. However, in some cases the police are not required to carry out the investigation unless the injured party demands that the offender is punished. Computer crimes usually fall within this category. A head of investigation is appointed for each criminal

[17] This is not an exhaustive list as there are several provisions in the Finnish Penal Code, which could also apply to the content related crimes.

[18] http://www.ficom.fi/fi/index.html

case to be investigated. The police are also required to notify a prosecutor for each criminal case that they are investigating whenever a person is suspected of an offence.

The following computer crime investigation measures are available:

8.4.1 Disclosure of data

The right of authorities to demand identification data for the purpose of preventing and uncovering crime is laid down in the Police Act and the Customs Act. When the data is needed for the purpose of investigating a completed crime, the right is laid down in the Coercive Measures Act.

In certain situations (e.g. when it is necessary to carry out their duties, or if they find that there are sufficient indications to suspect a crime has been committed), the Data Ombudsman and the Finnish Communications Regulatory authority are also entitled to request identification data, location data and even specific messages (the latter only in case of criminal computer mischief and interference).

8.4.2 Telecommunications interception and monitoring

The district court may grant the police a license to listen to and record messages, if there is reason to suspect the person of certain serious offences, as listed in the Coercive Measures Act. A license for telecommunications monitoring may be granted e.g. if there is reason to suspect the person of an offence against an IT system using a data terminal.

8.4.3 Restraint on alienation and seizure for escrow

The district court may impose a restraint on alienation on property that belongs to a person suspected with probable cause of an offence. A restraint on alienation may not cover more property than that corresponding to the applicable fine.

8.5 References (www.om.fi, www.finlex.fi)

- The Penal Code of Finland (39/1889) (Rikoslaki)
- The Criminal Procedure Act (689/1997) (Laki oikeudenkäynnistä rikosasioissa)
- The Data Protection Act (523/1999) (Henkilötietolaki)
- The Act on the Protection of Privacy in Electronic Communications (516/2004) (Sähköisen viestinnän tietosuojalaki)
- Act on classification of Audiovisual Programs (775/2000) (Laki kuvaohjelmien tarkastamisesta)
- The Pre-Trial Investigation Act (449/1987) (Esitutkintalaki)
- The Coercive Measures Act (450/1987) (Pakkokeinolaki)
- The Police Act (493/1995) (Poliisilaki)
- The Customs Act (1466/1994) (Tullilaki)

CHAPTER 9 Country Report: France

9.1 French legislation on computer crimes

France was one of the first European nations to draft specific cyber-crime provisions, through the Information Technology and Liberty Act (*Loi Informatique et Libertés)* of 1978, and more significantly the so-called Godfrain Act (*Loi Godfrain)* of 5 january 1988. The Godfrain Act updated the French penal code by introducing a section regarding the intrusion in information systems (articles 323-1 to 323-7). This section has been updated several times since its introduction. The most recent modification occurred through the Act of 21 June 2004 Reinforcing Trust in the Digital Economy (*Loi du 21 juin 2004 pour la Confiance dans l'Economie Numérique*).

Additionally, several other provisions have been adapted in the past few years to ensure their applicability in the information society, e.g. regarding fraud, the distribution of child pornography, commercial communications (including spam), and interception of private communications.

Specific provisions have also been introduced in the Penal Procedure Code, e.g. regarding encryption/decryption, communications monitoring, and data seizure.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another form of cyber-crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime
Malicious code	Article 323-2 Penal Code	Hindering the proper functioning of an information system	Imprisonment of 5 years and a fine of EUR 75,000.
	Article 323-3 Penal Code	Fraudulently introducing, modifying or deleting data in an information system	Imprisonment of 5 years and a fine of EUR 75,000.
	Article 323-1 Penal Code	Fraudulently penetrating or maintaining access to an information system	Imprisonment of 2 years and a fine of EUR 30,000. If data within the system is deleted or modified as a consequence of the penetration, or if the system's functioning is hindered, the punishment is imprisonment of 3 years and a fine of EUR 45,000
Denial of service	Article 323-2 Penal Code	Hindering the proper functioning of an information system	Imprisonment of 5 years and a fine of EUR 75,000.
	Article 323-3 Penal Code	Fraudulently introducing, modifying or deleting data in an information system	Imprisonment of 5 years and a fine of EUR 75,000.
Account compromise	Article 323-1 Penal Code	Fraudulently penetrating or maintaining access to an information system	Imprisonment of 2 years and a fine of EUR 30,000. If data within the system is deleted or modified as a consequence of the penetration, or if the system's functioning is hindered, the punishment is imprisonment of 3 years and a fine of EUR 45,000
	Article 323-3 Penal Code	Fraudulently introducing, modifying or deleting data in an information system	Imprisonment of 5 years and a fine of EUR 75,000.
	Article 313-1 Penal Code	Fraud: using a false name or false credentials to manipulate a person to hand over funds, goods, or to provide a service	Imprisonment of 5 years and a fine of EUR 375,000.

Intrusion attempt	Article 323-1 and 323-7 Penal Code	Preparatory measures in view of unauthorised access	Imprisonment of 2 years and a fine of EUR 30,000.
Unauthorised access to information	Article 323-1 Penal Code	Fraudulently penetrating or maintaining access to an information system	Imprisonment of 2 years and a fine of EUR 30,000. If data within the system is deleted or modified as a consequence of the penetration, or if the system's functioning is hindered, the punishment is imprisonment of 3 years and a fine of EUR 45,000
	Article 226-15 Penal Code	Intercepting, delaying or using another person's telecommunications messages in bad faith or installing devices designed for such interceptions	Imprisonment of 1 year and a fine of EUR 45,000. When the crime is committed by a public official or by a representative of a telecommunications service provider during the exercise of their functions: imprisonment of 3 years and a fine of EUR 45,000
Unauthorised access to transmissions	Article 226-15 Penal Code	Intercepting, delaying or using another person's telecommunications messages in bad faith or installing devices designed for such interceptions	Imprisonment of 1 year and a fine of EUR 45,000. When the crime is committed by a public official or by a representative of a telecommunications service provider during the exercise of their functions: imprisonment of 3 years and a fine of EUR 45,000
Unauthorised modification of information	Article 323-1 Penal Code	Fraudulently penetrating or maintaining access to an information system, resulting in the deletion or modification of data within the system	Imprisonment of 3 years and a fine of EUR 45,000
	Article 323-3 Penal Code	Fraudulently introducing, modifying or deleting data in an information system	Imprisonment of 5 years and a fine of EUR 75,000.
Unauthorised access to communication systems	Article 323-1 Penal Code	Fraudulently penetrating or maintaining access to an information system	Imprisonment of 2 years and a fine of EUR 30,000. If data within the system is deleted or modified as a consequence of the penetration, or if the system's functioning is hindered, the punishment is imprisonment of 3 years and a fine of EUR 45,000

	Article 226-15 Penal Code	Intercepting, delaying or using another person's telecommunications messages in bad faith or installing devices designed for such interceptions	Imprisonment of 1 year and a fine of EUR 45,000. When the crime is committed by a public official or by a representative of a telecommunications service provider during the exercise of their functions: imprisonment of 3 years and a fine of EUR 45,000
Spam	Article L. 34-5 of the Postal and Telecommunications Code, and article L. 121-20-5 of the Consumer Code	Directly contacting prospective customers using an automated calling device, fax or e-mail without their prior consent	A fine of EUR 750 per illegitimately sent message
	Article 226-16 Penal Code	Foregoing formalities before automatically processing data (such as registering the processing activities with the national data protection authority, CNIL)	Imprisonment of 5 years and a fine of EUR 300,000
	Article 226-18 Penal Code	Fraudulently, illegitimately or unfairly collecting personal data	Imprisonment of 5 years and a fine of EUR 300,000

9.2 Law enforcement bodies

9.2.1 Police (www.interieur.gouv.fr/rubriques/c/c3_police_nationale)

The national police (consisting of local police and gendarmerie) consist of a number of administrations, including the Central Administration of Judicial Police (*direction centrale de la police judiciaire*). Depending on the function of the Judicial Police's public officials, their competence can span several French administrative territories, or it can even be national.

The Central Office for the Fight against ICT crime (*Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.))* is a subsection of the Judicial Police, and specialises in cyber-crime. Their task is to provide operational and technical coordination of cyber-crime investigations on a national level. They may also undertake any necessary research activities themselves, thus supporting local police, *gendarmerie,* and the General Administration for Competition, Consumption and Fraud Repression (*la Direction Générale de la Concurrence, de la Consommation et de la répression des fraudes*) in their investigations.

O.C.L.C.T.I.C. is also the international contact point for any cross-border cyber-crime activities, and liaises closely with a number of related French administrations, such as:

- The Territorial surveillance administration (*Direction de la surveillance du territoire*), which is in charge of investigations regarding hacking cases against high security or national defence systems.
- The National division for infractions against persons and goods (*Division nationale de répression des atteintes aux personnes et aux biens - DNRAPB*) is in charge of investigating infractions involving minors and involving press crimes on the Internet.
- In 1998, the Department for the fight against cyber-crime (*Département de lutte contre la cybercriminalité*) was created as a subsection of the Technical service of criminal investigations *(service technique de recherches judiciaires et de documentation - STRJD)*. This service is also competent for investigating illegal and harmful content found on the Internet.
- A subdivision of the Institute of criminal investigations of the gendarmerie (*Institut de recherche criminelle de la gendarmerie - IRCGN*), namely the Criminal division for Engineering and ICT (*Division criminalistique "ingénierie et numérique")* can assist in any technical research activities.
- Additionally, the Paris police department has erected an Internet group within the Brigade for the protection of minors (*groupe Internet de la Brigade de Protection des Mineurs - BPM*) and within the Brigade for investigation of ICT fraud (*Brigade d'enquêtes sur les fraudes aux technologies de l'information - BEFTI*).

9.2.2 Courts (www.legifrance.gouv.fr)

The court most likely to deal with computer crime is the Correctional court (*Tribunal correctionnel*), a subsection of the Court of First Instance (*Tribunal de Grande Instance*). Against its decisions, appeal can be lodged with the Court of Appeal, criminal chamber (*Cour d'appel, chambre des appels correctionnels*). The Supreme Court (*Cour de Cassation*) only hears points of law. Proceedings on the merits of the case are always preceded by an inquiry under the supervision of the investigating magistrate.

9.3 Reporting

9.3.1 Competent authorities

The *O.C.L.C.T.I.C.* is the main competent investigating body, and the national contact point for cyber-crime incidents. Incidents can thus be reported to the O.C.L.C.T.I.C. directly, or to the public prosecutor (*Procureur de la République*) of the region of the victim's domicile. Detailed contact information is available on the

following page: http://www.interieur.gouv.fr/rubriques/divers/contacts/cybercriminalite

Depending on the nature and localisation of the incident other organisations may be involved, such as the National division for infractions against persons and goods (*Division nationale de répression des atteintes aux personnes et aux biens - DNRAPB*), the Technical service of criminal investigations *(service technique de recherches judiciaires et de documentation - STRJD)*, and/or the Institute of criminal investigations of the gendarmerie (*Institut de recherche criminelle de la gendarmerie - IRCGN*).

9.3.2 Contact details

Central Office for the Fight against ICT crime
(O.C.L.C.T.I.C.)
MINISTERE DE L'INTERIEUR
Direction Centrale de la Police Judiciaire
Sous-Direction des Affaires Economiques et Financières
Rue des Saussaies 11
75800 Paris Cedex 08
T : +33 1 40 07 69 49
F : +33 1 40 07 29 76
E : oclctic@interieur.gouv.fr
URL: www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic
Languages: French

National Commission of ICT and Liberties
(Commission Nationale de l'Informatique et des Libertés)
Rue St-Guillaume 21
75340 Paris cedex 07
T: +33 1 53 73 22 22
E: only postal communication
URL: www.cnil.fr
Languages: French

9.3.3 Other reporting mechanisms

As mentioned above, ICT incidents can be reported online directly to O.C.L.C.T.I.C. through their contact site (http://www.interieur.gouv.fr/rubriques/divers/contacts/mail_cybercriminalite/contact), or through e-mail (oclctic@interieur.gouv.fr). Alternatively, the public prosecutor of the victim's region of domicile can be contacted online, through http://www.justice.gouv.fr/region/consult.php

However, a number of alternative reporting mechanisms exist for specific crimes.

- In September 1997, the French ISP Association AFA (www.afa-france.com) established a reporting site, Pointdecont@ct.net (www.pointdecontact.net). The site functions as a hotline against on-line child pornography, racist content or any other content that violates human dignity. It also functions as a general information portal, where information about a number of other issues such as spam can be found. AFA was also one of the founding members of the European INHOPE network, so that Pointdecont@ct.net maintains close links to a number of similar European contact points. Reports can be filed anonymously through the following page: http://www.pointdecontact.net/contact.asp

- Additionally, child pornography can be reported on a separate website controlled by the French government: www.internet-mineurs.gouv.fr. The main difference with Pointdecont@ct.net is that the reports filed through www.internet-mineurs.gouv.fr are automatically registered in a database managed by O.C.L.C.T.I.C., whereas Pointdecont@ct.net first verifies the illegal or harmful character of the reported contents, before deciding whether or not to file a report with the competent authorities.

9.4 Forensics

Like many European continental states, France has a free or informal system of evidence. Thus, offences may typically be proven by any means of proof, including electronic proof, and the acting judge is free to decide upon the value of the evidence in accordance with his inner convictions.

Specific investigation procedures (such as seizures, searches, ordering the involvement of experts, etc.) are regulated by the Penal Procedure Code (*Code de Procédure Pénale*).

After an incident is discovered or reported, an investigating magistrate (*juge d'instruction*) will typically be appointed. He will lead the pre-trial investigation, assisted by the institutions mentioned above (O.C.L.C.T.I.C., D.S.T., D.N.R.A.P.B., I.R.C.G.N. and I.R.C.G.N.) if necessary. For certain investigation measures (such as ordering searches) the examining magistrate has exclusive competence. In some cases, a prosecutor or judge will use a civil expert to carry out the investigation.

The following specific computer crime investigation measures are available:

9.4.1 Search and seizure

Article 94 of the Penal Procedure Code was updated in 1991 and in 2004 to allow searches to be conducted in any place where objects or electronic data (*données électroniques*) can be found, if this is useful to reveal the truth. This would include searches through computer systems or networks.

Article 97 of this Code provides details on how this is to take place. An inventory of all seized objects, documents or data must immediately be made, and they must all be sealed. Data can be seized by either seizing the physical carrier itself (e.g. a hard disk), or by making a copy of the data. When a copy is made, the original data can be erased if the possession or use of the data is illegal or dangerous.

The investigating magistrate may also order any person or organisation holding specific electronic data that could be of interest to the investigation, to reveal this information to him (article 99-3 of the Penal Procedure Code)

9.4.2 Ordering the interception of communication

The investigating magistrate may order telecommunications to be recorded, registered or transcribed if a person is suspected of a serious crime (with a possible punishment of two

years imprisonment or more) and if the importance of the information warrants it (article 100 and following of the Penal Procedure Code.

9.4.3 Ordering the participation of experts

The investigating magistrate may order persons who have the necessary expertise to assist in his investigations. An expertise may also be requested by the parties involved (article 156 and following of the Penal Procedure Code). The expert is required to report neutrally on the questions he was asked within the confines of his mandate. Multiple experts can be appointed to explore one question, if required.

9.4.4 Ordering the decryption of information

The investigating magistrate may order persons who have the necessary information on the decryption of relevant data to decrypt this data (article 230 of the Penal Procedure Code). Refusal to provide a decryption key is punishable according to article 434-15-2 of the Penal Code.

9.5 References (http://www.legifrance.gouv.fr/)

- Penal Code (1992) and Penal Procedure Code [1958]
- Information Technology and Liberty Act (*Loi Informatique et Libertés)* of 1978
- Law of 5 January 1998 regarding ICT fraud (*Loi n°88-19 relative à la fraude informatique*)
- Law of 15 November 2001 regarding daily security (*Loi n°2001-1062 relative à la sécurité quotidienne*)
- Law of 18 March 2003 regarding national security (*Loi n°2003-239 pour la sécurité intérieure*)
- Law of 3 March 2004) adapting the organisation of justice to evolutions in crime (*Loi n°2004-204 portant adaptation de la justice aux évolutions de la criminalité*)
- Law of 21 June 2004 reinforcing trust in the digital economy (*Loi n°2004-575 pour la confiance dans l'économie numérique*)
- Law of 9 July 2004 regarding electronic communications and audiovisual communication services (*Loi n°2004-669 relative aux communications électroniques et aux services de communication audiovisuelle*)

CHAPTER 10 Country Report: Germany

10.1 German legislation on computer crimes[19]

Offences against the Confidentiality, Integrity and Availability of information are regulated in the German Criminal Code (StGB). There are mainly six special articles dealing with these sorts of offences:

§ 202 a StGB: Data Espionage

§ 303 a StGB: Alteration of Data

§ 303 b StGB: Computer Sabotage

§ 263 a StGB: Computer Fraud

§ 269 StGB: Falsification of Legally Relevant Data

§ 270 StGB: Deception in Legal Relations through Data Processing

Illicit content is mainly regulated in three articles of the German Criminal Code:

§ 130 StGB: Incitement of the People

§ 131 StGB: Glorification of Violence

§ 184 StGB: Dissemination of Pornographic Writings

[19] German law does not generally specify the amount of a fine for any given provision. Thus, the table below does mention whether or not a specific provisions prescribes a fine, but not the exact sum.

Relevant Incidents	Applicable provision	Description	Sanction
Target fingerprinting	None as such	Only a preparatory act (attempt to commit another form of cyber-crime)	Not punishable as such.
Malicious code	None as such	Only a preparatory act (attempt to commit another form of cyber-crime, for instance: Unauthorized access to information, unauthorized modification of information or unauthorized access to communication systems)	Not punishable as such.
Denial of service	Article 303 a StGB	Unlawfully deleting, suppressing, rendering or altering data	Imprisonment up to 2 years or a fine
	Article 303 b StGB	Committing the crime described in article 303 a StGB, where the affected data processing is vitally important for another business, enterprise or public authority	Imprisonment up to 5 years or a fine
Account compromise	None as such	Only a preparatory act (attempt to commit another form of cyber-crime, for instance: Unauthorised access to information, unauthorised modification of information or unauthorised access to communication systems)	Not punishable as such.
Intrusion attempt	None as such	Only a preparatory act (attempt to commit another form of cyber-crime, for instance: Unauthorised access to information, unauthorised modification of information or unauthorised access to communication systems)	Not punishable as such.

Unauthorised access to information	Article 202 a StGB	Unauthorised obtaining of data not meant for the offender and specially protected against unauthorised access	Imprisonment up to 3 years or a fine
Unauthorised access to transmissions	Article 303 a StGB	Unlawfully deleting, suppressing, rendering or altering data	Imprisonment up to 2 years or a fine
	Article 303 b StGB	Committing the crime described in article 303 a StGB, where the affected data processing is vitally important for another business, enterprise or public authority	Imprisonment up to 5 years or a fine
Unauthorised modification of information	Article 303 a StGB	Unlawfully deleting, suppressing, rendering or altering data	Imprisonment up to 2 years or a fine
	Article 303 b StGB	Committing the crime described in article 303 a StGB, where the affected data processing is vitally important for another business, enterprise or public authority	Imprisonment up to 5 years or a fine
Unauthorised access to communication systems	Article 303 a StGB	Unauthorized modification of settings of another communication system by unlawfully deleting, suppressing, rendering or altering data	Imprisonment up to 2 years or a fine
	Article 303 b StGB	Unauthorised modification of settings of another communication system by committing the crime described in article 303 a StGB, where the affected data processing is vitally important for another business, enterprise or public authority	Imprisonment up to 5 years or a fine

	Article 263 a StGB	If a person damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorized influence on the workflow with the intent of obtaining an unlawful material benefit	Imprisonment up to 5 years or a fine
	Article 265 a StGB	If a person uses a public telecommunication network without the intent of paying the fee	Imprisonment up to 1 year or a fine
Spam	None as such	No criminal liability, only civil liability (Claim for damages, Claim for injunction, Infringement of the Unfair Competition Act (UWG)) An Anti-Spam Act is subject of discussions.	

10.2 Law enforcement bodies

10.2.1 Police (www.polizei.de)

German police consists of a Federal Criminal Police Office (*Bundeskriminalamt*-BKA: www.bka.de) and the police forces in the 16 federal states (*Laender*).

In general, the individual 16 Laender are responsible for law enforcement and public security. The police forces under Laender jurisdiction include the general police which deals with public order and minor offences and the criminal police which deals with more serious offences.

The BKA is the central office for police information and intelligence and for the cooperation between the Federation and the Laender in all criminal police matters. Furthermore, it is the national central bureau for the International Criminal Police Organization (ICPO-Interpol).

10.2.2 Courts

The courts most likely to deal with computer crimes are the District Courts (*Amtsgerichte*), criminal section. Against its decisions, appeal can be lodged to the *Landgericht*. The *Oberlandesgericht* only hears points of law.

10.3 Reporting

10.3.1 Competent authorities

Generally computer crimes should be reported to the police of the individual state. Nevertheless a computer crime can also be reported to any other police office or the BKA who will forward the report to the responsible police authority.

10.3.2 Contact details

Federal Criminal Police Office *(Bundeskriminalamt)*
65173 Wiesbaden
T : +49 611 550
F : +49 611 5512141
E: info@bka.de
URL: www.bka.de

National Privacy Protection Commission
(*Bundesbeauftragten für den Datenschutz*)
Husarenstraße 30
53117 Bonn
T: +49 1888 7799 0
F: +49 1888 7799 550
E: poststelle@bfd.bund.de
URL: www.bfd.bund.de
Languages: German, French, English

10.3.3 Other reporting mechanisms

The most important authority for securing information systems and networks is the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* - www.bsi.de). The purpose of this e-security platform is to react quickly and accurately in case of virus attacks. Internet users can subscribe to a free mailing list to receive latest information on circulating computer viruses (www.bsi.bund.de/certbund/infodienst/index.htm). There is also a hotline available to report viruses and to get information:

Bundesamt für Sicherheit in der
Informationstechnik
Referat I 2.4
Postfach 200363
53133 Bonn
+49 1888 9582 444
e-mail: antivir@bsi.bund.de

There are also several alert mechanisms for content related crimes.

Illicit content – Child pornography, racism and the promotion of games of chance are examples of explicitly forbidden Internet content in Germany.

Harmful content – Content that can generally be harmful to Internet users, in particular minors, is regulated by the Protection of Minors in the Media Treaty (*Jugendmedienschutz-Staatsvertrag* (JMStV)).

- A special alert mechanism for illicit or harmful information on the Internet exists on the website of Jugendschutz.net (www.jugendschutz.net/hotline/index.html). Internet users and ISPs can notify any supposed illicit or harmful information on the Internet via an e-mail (hotline@jugendschutz.net) or fill in a form directly on the website. Notifications can be done on an anonymous basis and should contain as much useful information as possible, such as the URL of the website or the full heading of a news item.
- Another alert mechanism for child pornography has been set up by the Federal Criminal Police Office. A Central Unit for Child Pornography (*Zentralstelle Kinderpornografie* - KIPO) was established. Useful information on this issue is posted on the BKA website (www.bka.de) with the purpose of informing people on how to behave in case of detecting child pornography in the Internet. Child pornography can be reported to the BKA (info@bka.de) that will forward the report to the responsible police authority.
- Also a regime of self-regulation of the ISPs was established: the Voluntary Self-Control for Multimedia Service Providers (*Freiwillige Selbstkontrolle Multimedia-Diensteanbieter* - www.fsm.de). Illicit and harmful content can be reported to this organisation. Users can fill in a form directly on the website or send an e-mail to hotline@fsm.de. This service is also available in English. Notifications cannot be done on an anonymous basis.

10.4 Forensics

All kinds of evidence may be submitted. Electronic evidence is admitted as a common form of evidence. The more authentic the evidence, the easier it will be to convince a judge during proceedings.

When confronted with computer crime (through a complaint or discovery by the police), the responsible police authority will carry out the initial inquiry and forensics under the supervision of the public prosecutor. In some cases, such as searching of a house or building or data seizure, the police needs a special warrant issued by a judge. In urgent cases it can also be issued by a prosecutor.

The following specific computer crime investigation measures are available:

10.4.1 Data seizure

Due to the immaterial nature of data only the storage devices of data can be seized (Articles 98, 94 StPO). According to Article 110 StPO only prosecutors and not the police are allowed to examine the suspicious data.

10.4.2 Network searching

Network searching is not regulated explicitly in the StPO. The provisions about the searching of a house or building (Article 102 StPO) are applicable in an analogue way. Therefore a search warrant issued by a judge, or in urgent cases by a prosecutor, is necessary (Article 105 StPO).

10.4.3 Monitoring of e-mail traffic

All investigation measures concerning e-mail traffic have to comply with the secrecy of telecommunications (Art. 10 Basic Law (German Constitution). Therefore the monitoring of e-mail traffic is only allowed in case of certain severe offences that are explicitly mentioned in Article 100 a StPO, such as offences against national security or defense, murder, genocide, robbery etc. Also in this case a warrant issued by a judge or in urgent cases by a prosecutor is necessary (Article 100 b StPO).

10.4.4 Involvement of experts

The prosecutor may order persons who have the necessary expertise to provide information on the working of the relevant informatics system or on how to get access to the relevant electronic data. For instance the network administrator may be asked to provide a password or to provide information on the security technique adopted for the system.

10.5 References (http://bundesrecht.juris.de/bundesrecht/gesamt_index.html)

- Basic Law of the Federal Republic of Germany (1949) last amended 26.07.2002 (*Grundgesetz*-GG)
- Penal Code (1871) last amended 24.03.2005 (*Strafgesetzbuch*-StGB)
- Code of Criminal Procedure (1950) last amended 22.03.2005 (*Strafprozessordnung*-StPO)
- Federal Data Protection Act (1990) last amended 14.01.2003 (*Bundesdatenschutzgesetz*-BDSG)
- Telecommunications Act (2004) last amended 14.03.2005 (*Telekommunikationsgesetz*-TKG)
- Teleservices Act (1997) last amended 14.12.2001 (*Gesetz über die Nutzung von Telediensten*-TDG)
- Unfair Competition Act (2004) (*Gesetz gegen den unlauteren Wettbewerb*-UWG)

- Protection of Minors in the Media Treaty (2004) (*Jugendmedienschutz-Staatsvertrag*-JMStV)

CHAPTER 11 Country report - Greece

11.1 Greek legislation on computer crimes

In 2001 the Greek constitution which had been decreed in 1975 was revised. The new provisions include several sections which are relevant to the information society and new technologies. In the revised Greek Constitution a new article 5a was added, which explicitly gives every citizen, regardless of nationality, the right to access data. Restrictions to the above right can be imposed by the State only to combat crime.

Specific Legislation

In Greece, there is no separate legislation concerning crimes committed through the Internet. The Greek prosecuting authorities and the Greek courtrooms treat these criminal acts depending on legal provisions in the Greek Criminal Code.

Specifically, the Criminal Code includes provisions 386A (computer fraud) and 370B and 370 (unlawful access) that deal with committing crimes using a computer (all added to the Criminal Code through articles 5, 3 and 4 respectively of Act 1805/1988). Combined with the general provisions about the protection of honour, property, estate, memorandum, child pornography and a specific law for the protection of copyright, these make up the legislation for the proper legal protection of citizens against criminal ICT acts.

To the maximum possible extent, the Greek legislator has equated committing crimes through the Internet to performing any other criminal act through a written document or in the press. In the last 5 years, a more specific legislative framework concerning the above crimes has not been created, with the only exception being the new provision regarding child pornography (Act 3068/2002). According to the new article 348A of the Criminal Code, anyone who uses the internet in order to distribute images of a child pornographic nature is punished with imprisonment of up to 10 years.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another form of cyber-crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime. A lesser punishment is imposed if the felony or the misdemeanour is not completed (Article 83 Criminal Code)
Malicious code	Article 381 Criminal Code	Intentionally damaging foreign property (including electronic data), wholly or in part, or in any other way preventing its use.	Imprisonment of up to two years.
	Article 386A Criminal Code	Intentionally and unlawfully attempting to enrich oneself or another, by causing damage to another through affecting computer data either by incorrectly executing a computer programme, or by using wrong or incomplete data, or by causing damage to the data in any other way.	Imprisonment of up to two years. If the offender commits fraud (by using malicious codes) as a profession or habitually and the damage is valued over EUR 15,000, or if the damage caused by the malicious code is over EUR 73,000, then the maximum penalty is increased to imprisonment of up to ten years.
Denial of service	Article 381 Criminal Code	Intentionally damaging foreign property (including electronic data), wholly or in part, or in any other way preventing its use.	Imprisonment of up to two years.
	Article 370 C §2 Criminal Code	Unlawful access to data recorded in a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder.	Imprisonment of up to three months or a fine of EUR 29 to 15,000.

Account compromise	Article 370 C §2 Criminal Code	Unlawful access to data recorded in a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder.	Imprisonment of up to three months or a fine of EUR 29 to 15,000.
	Article 370 B Criminal Code	Unauthorised access and maintenance of access to a computer system's secret data.	Imprisonment between 3 months and 5 years, if the data is secret.
Intrusion attempt	Article 370 C §2 Criminal Code	Unlawful access to data recorded in a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder.	Imprisonment of up to three months or a fine of EUR 29 to 15,000. A lesser punishment is imposed if the felony or the misdemeanour is not completed (Article 83 Criminal Code)
	Article 370 B Criminal Code	Unauthorised access and maintenance of access to a computer system's secret data.	Imprisonment between 3 months and 5 years, if the data is secret. A lesser punishment is imposed if the felony or the misdemeanour is not completed (Article 83 Criminal Code)
Unauthorised access to information	Article 370 C §2 Criminal Code	Unlawful access to data recorded in a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder.	Imprisonment of up to three months or a fine of EUR 29 to 15,000.

		If the offender is in the service of the legal holder of the data, the act describe above shall only be punishable if it has been explicitly prohibited by an internal regulation or by a written decision by the holder or by a competent employee.	Imprisonment of up to three months or a fine of EUR 29 to 15,000.
Unauthorised access to transmissions	Article 370 §1 Criminal Code	Unlawfully and with the intent to obtain knowledge of its contents opening of a sealed document, or violating another's privacy using any other means by reading, rewriting or otherwise copying a letter or a document.	Imprisonment of up to one year.
	Article 370 A Criminal Code	Unauthorised access to private telephone exchanges and voicemail systems.	Imprisonment between ten days and five years.
Unauthorised modification of information	Article 370 C §2 Criminal Code	Unlawful access to data recorded in a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder.	Imprisonment of up to three months or a fine of EUR 29 to 15,000.
	Article 381 Criminal Code	Intentionally damaging foreign property (including electronic data), wholly or in part, or in any other way preventing its use.	Imprisonment of up to two years.

Unauthorised access to communication systems	Article 370 C §2 Criminal Code	Unlawful access to data recorded in a computer or in the external memory of a computer transmitted by telecommunication system, especially in violation of prohibitions or of security measures taken by the legal holder.	Imprisonment of up to three months or a fine of EUR 29 to 15,000.
		If the offender is in the service of the legal holder of the data, the act describe above shall only be punishable if it has been explicitly prohibited by an internal regulation or by a written decision by the holder or by a competent employee.	Imprisonment of up to three months or a fine of EUR 29 to 15,000.
	Article 370 §1 Criminal Code	Unlawfully and with the intent to obtain knowledge of its contents opening of a sealed document, or violating another's privacy using any other means by reading, rewriting or otherwise copying a letter or a document.	Imprisonment of up to one year.
	Article 370 A Criminal Code	Unauthorised access to private telephone exchanges and voicemail systems.	Imprisonment between ten days and five years.
Spam	No applicable provision.	The use of electronic mail for advertising purposes without the prior, free, specific and informed consent of the addressee of the messages is not forbidden by the Greek Criminal Code or any other penal law.	None

	Article 348 §3 Criminal Code	Professionally or for financial gain, by advertisements, pictures, phone numbers, electronic mails or by any mean acts to facilitate indecency between adults and a person under 18 years of age.	Imprisonment between ten days and five years and a fine up to EUR 100,000

11.2 Law enforcement bodies

11.2.1 Police (www.ydt.gr)

The Greek Police is charged with the investigation of crimes. A special service within the Greek Police, the Prosecution Force of Electronic Crime (*Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος*), is commissioned to investigate Internet crimes. The Hellenic Data Protection Authority (*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*), which is an independent institution, not being a part of the Government although it is a state authority, is commissioned to protect citizens against unlawful use of their personal data.

11.2.2 Courts (www.ministryofjustice.gr/)

The administration of justice falls under the competence of the Ministry of Justice. There are three courts: civil, administrative and criminal. The civil and administrative courts are organised in the same way, but the criminal courts are classified in three levels according to the type of offence to be tried:

(I.) Contraventions Court (similar to police court or tribunal de simple police – *Πταισματοδικείο*): competent for any illegal act referred to as a contravention (*πταίσμα*), punishable by jailing.

(II.) Offenses Court (similar to magistrate's court or tribunal correctionnel - *Πλημμελειοδικείο*): competent for any illegal act referred to as an offense (*πλημμέλημα*), punishable by imprisonment.

(III.) Felonies Court (similar to court of assizes or cour d'assisses - *Κακουργιοδικείο*): competent for any illegal act referred to as a felony ('κακούργημα'), punishable by confinement in a penitentiary.

The penal courtrooms undertake the trial of punishable actions. The categories of penal courtrooms are distinguished according to the anticipated punishments: imprisonment ranging from 5 years up to 20 years or permanent; imprisonment from 10 days up to 5 years; and jailing from 1 day up to 1 month.

11.3 Reporting

11.3.1 Competent authorities

Law enforcement is organised by the Ministry of Public Security. Policing is carried out by the Hellenic Police (*Ελληνική Αστυνομία*). Each crime is prosecuted either after the victim has pressed charges or at the District Attorney's own initiative.

The Ministry of Public Security - Hellenic Police can be contacted at the following coordinates:

4 P. Kanellopoulou St.,
GR-10177 Athens
T: +30 210 6977000
F: +30 210 6912661 or +30 210 6920487
http://www.ydt.gr/

11.3.2 Contact details

Information Technology Crimes
Alexandras Ave. 173
GR-115 22 Athens
Greece
T: +30 210 6456440
F: +30 210 6430238

Hellenic Data Protection Authority,
Kifisias Av. 1-3
PC 115 23, Ampelokipi, Athens
T: +30 210 6475601
F: +30 210 6475628
E: contact@dpa.gr
URL: www.dpa.gr

11.3.3 Other reporting mechanisms

Online child pornography can be reported via www.hamogelo.gr/, which provides contact information through phone or SMS. No other reporting mechanisms exist.

11.4 Forensics

The Greek legislator considered it unnecessary to provide specific legislation for most investigative measures. However, it did see fit to amend article 13 of the Criminal Code (through article 2 of Act 1805/1988), which now states that "A document includes any means which is used in a computer or a peripheral computer memory, in an electronic, magnetic or other way, to enter, save, produce or reproduce data, which cannot be read directly, as well as any magnetic, electronic or other material on which any information, icon, symbol or sound is entered, either independently or combined, as long as those means and materials are predestined or suitable to prove facts that have legal importance". As such, Greece is one of the few countries that legally define requirements for electronic documents in legal procedures.

One of the basic principles of criminal investigation – not only for cyber crimes, but for any crime – is the principle of proportionality, i.e. the prohibition of using means which are considered unnecessary or excessive for the purposes of the prosecutions authorities. Any measure thus requires (in principle) that an order is issued by an inquisitor (investigator) or by the court that is examining the case. During the investigation the accused may consult an attorney and observe the legality of the proceedings.

Seizures are in practice performed by the policemen who are conducting the investigation. They may seize the corpus delicti (such as the personal computer of the accused), as specified in the public prosecutor's order, and take it to a forensic laboratory. Here specialists investigate the software and any other element that can shed light on the crime and provide proof of guilt or innocence.

11.5 References

- Greek Criminal Code, 1950, (*Ελληνικός Ποινικός Κώδικας*)
- Act 1805/1988, "Amending some provisions of the Criminal Code" (*Νόμος 1805/1988 Τροποποίηση διατάξεων του ποινικού κώδικα*)
- Act 3068/2002, "Trafficking of human beings, sexual exploitation and child pornography and financial utilisation in general of sexual life, and assistance to the victims of such crimes" (*Νόμος 3064/2002 «καταπολέμηση της εμπορίας ανθρώπων, των εγκλημάτων κατά της γενετήσιας ελευθερίας, της πορνογραφίας ανηλίκων και γενικά κατά της οικονομικής εκμετάλλευσης της γενετήσιας ζωής, και αρωγή στα θύματα αυτών των εγκλημάτων»*)

CHAPTER 12 Country report – Hungary

12.1 Hungarian legislation on computer crimes

Taking into consideration the increasing number of computer-related offences, the Council of Europe decided to elaborate an international convention. In November 2001, the Convention on Cybercrime was adopted by the Council of Europe in Budapest, Hungary. The Hungarian Parliament implemented these measures and amended the Criminal Code accordingly. Section 22, 57 and 58 of the Act no. CXXI of 2001 introduced specific computer-related criminal offences into the Hungarian Criminal Code (illegal access, data manipulation, system interference, misuse of devices, informatics forgery, informatics fraud and illegal interception). Beside these amendments, there are two other categories of computer-related offences: first, "content-related crimes" like child pornography and second, the infringement of copyright and related rights in the Hungarian Criminal Code. Furthermore, the Hungarian Criminal Procedure Act (Act No. XIX of 1998) provides for the interim and coercive measures imposing data retention obligations on operators and service providers of electronic communication. (Section 158/a).

In addition, specific governmental decrees deal with the breach of obligations related to electronic communication.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Section 178 (1)-(3) Criminal Code	Violation of the secrecy of correspondence by means of telecommunication equipment	For the main offence: fine[20]. In case of aggravated circumstances : - imprisonment of one year, public labour or fine, if the crime is committed by abusing an occupation or public mandate; - imprisonment of 2 years, if the crime causes considerable injury of interest. - imprisonment of 3 years if the crime is committed by abusing an occupation or public mandate and causes considerable injury of interest
	Section 178/A (1) d and 178/A (2)-(3), Criminal Code	Interception and recording of private data or transmitted content by electronic communication equipment or computer system with the aim to gather information on private secret (without the agreement of the parties involved)	Imprisonment of up to five years. If the crime is committed under special circumstances (pretending official procedure, for business purpose, in alliance with other criminals or causing significant damage) the sanction is imprisonment between 2 years and 8 years
Malicious code	Section 300/C (2) b, Criminal Code	Inputting, transmitting, damaging, deleting, deteriorating, altering electronic data causing the malfunctioning of the computer system	Imprisonment up to two years, public labour or a fine
Denial of service	Section 300/C § (2) b, Criminal Code	Causing the malfunctioning of a computer system by introducing, altering, deleting, or modifying data in a computer system or through other action	Imprisonment of up to 2 years, public labour or fine

[20] Fines are determined for all offences under Section 51, §2 of the Criminal Code, which states: "The minimum and the maximum amount of the fine shall be equal to thirty days' and five hundred forty days' items, respectively. The amount of one day's item shall be no less than one hundred and no more than twenty thousand HUF."

Thus, all fines range between HUF 3,000 and 10,800,000 (approx. EUR 12 to 43,200).

	Section 300/C § (3) b, Criminal Code	For the purpose of gaining illegal benefit introducing, transmitting, altering, or deleting data processed, stored, or transmitted in the computer system or with any other action causing the malfunctioning of a computer system, thus causing damage	Imprisonment of up to three years (The upper limit of the imprisonment depends of the extent of the damage)
Account compromise	Section 300/C § (1) Criminal Code	Unauthorised access and maintenance of access to a computer system by outsiders, even without the intention to cause harm	Imprisonment of up to 1 year, public labour or fine
Intrusion attempt	Section 300/E. § (1) Criminal Code	Compromising or defrauding the integrity of a computer protection system or device.	Imprisonment of up to 2 years, public labour or fine
	Section 300/C § (1) Criminal Code	Preparatory measures of account compromise	Up to one year of imprisonment, but the judge has more discretion to decrease the punishment
Unauthorised access to information	Section 178/A (1) d, Criminal Code	Interception and recording of private data or transmitted content by electronic communication equipment or computer system with the aim to gather information on private secret (without the agreement of the parties involved)	Imprisonment of up to five years. If the crime is committed under special circumstances (pretending official procedure, for business purpose, in alliance with other criminals or causing significant damage) the sanction is imprisonment between 2 years and 8 years
Unauthorised access to transmissions	Section 178/A (1) d, Criminal Code	Interception and recording of private data or transmitted content by electronic communication equipment or computer system with the aim to gather information on private secret (without the agreement of the parties involved)	Imprisonment of up to five years. If the crime is committed under special circumstances (pretending official procedure, for business purpose, in alliance with other criminals or causing significant damage) the sanction is imprisonment between 2 years and 8 years

Unauthorised modification of information	Section 300/C § (2) b, Criminal Code	Causing the malfunctioning of a computer system by introducing, altering, deleting, or modifying data in a computer system or through other action	Imprisonment of up to 2 years, public labour or fine
	Section 300/C § (3) b, Criminal Code	For the purpose of gaining illegal benefit introducing, transmitting, altering, or deleting data processed, stored, or transmitted in the computer system or with any other action causing the malfunctioning of a computer system, thus causing damage	Imprisonment of up to three years (The upper limit of the imprisonment depends of the extent of the damage)
Unauthorised access to communication systems	Section 300/C § (1) Criminal Code	Unauthorised access and maintenance of access to a computer system by outsiders, even without the intention to cause harm	Imprisonment of up to one year, public labour or fine
Spam	Section 14§ (1) of Act no 108 of 2001 on electronic commercial services and services related to information society	The use of electronic mail for advertising purposes without the prior, free, specific and informed consent of the addressee of the messages is forbidden.	Fine imposed by the Consumer Protection Authority

12.2 Law enforcement bodies

12.2.1 Police (http://web.b-m.hu/police/index.html)

The Hungarian police system is structured in three levels: the National Police Office (*Országos Rendőr Főkapitányság*), the High Police Offices (*rendõrfõkapitányságok*) of the counties (19 county and 1 metropolitan) and the municipal police offices. The Directorate General of Communications and Prevention (*Kommunikációs és Megelõzési Főigazgatóság*) is subordinated to the National Police Office. This department consists of several working groups including the Internet Screening Group ("*Internet Figyelő Csoport*"). This group was created in February 2000 in order to perform the duties regarding the internet imposed on the police by law. The supervision of illegal content on the Internet falls within their competence, as well as the investigation of reports

related to offences of illegal access, data manipulation, system interference, misuse of devices, informatics forgery, informatics fraud and illegal interception.

12.2.2 Hungarian Customs and Finance Guard (http://vam.gov.hu/welcomeEn.do)

The Hungarian Customs and Finance Guard (*Vám- és Pénzügyőrség*) has limited investigative powers related to computer offences. The Directorate General of Criminal Affairs *(VP Központi Bûnüldözési Parancsnoksága*) may conduct investigation in case of the following offences: infringement of copyright and related rights – by unauthorized access, informatics forgery, informatics fraud. Its competence is not exclusive in the sense that the police also holds the power to investigate.

12.2.3 The Prosecutors Service (http://www.mklu.hu/cgi-bin/index.pl?lang=en)

The prosecutors (*ügyészség*) have a general power to supervise all criminal investigations, as well as the power to take over the investigation from other investigating bodies. Under section 28 and seq. of the Criminal Procedure Act, the prosecutor also acts as the public accuser.

When the investigating authority conducts an investigation or certain investigative actions independently, the prosecutor supervises the procedure and ensures that the persons participating in the procedure can assert their rights. With this in view, the prosecutor:

- may order an investigation, assign the investigating authority to conduct the investigation, and may instruct the investigating authority to perform – within the its own geographical jurisdiction – further investigative actions or further investigation, or to conclude the investigation within the deadline designated by the prosecutor;

- may be present at any investigative action, and may examine or send for the documents produced during the investigation;

- may amend or repeal the decision of the investigating authority, and shall consider the complaints received against the decision of the investigating authority;

- may reject the complaint, terminate the investigation and order the investigating authority to terminate the investigation;

- may refer the proceedings in his own competence.

In the event that the prosecutor conducts the investigation, he may instruct any investigating authority to perform an investigative action.

12.2.4 Courts (http://www.birosag.hu)

The court of first instance dealing with computer crime is the circuit court ("*helyi bíróság*"), located in most towns and cities. Appeal may be lodged and legal remedies may be granted at second instance by the county courts (*"megyei bíróság", Fővárosi Bíróság*), in limited cases, extraordinary remedies may be granted by the Court of Regions ("*Ítélőtábla"*).

12.3 Reporting

12.3.1 Competent authorities

The Data Protection and Freedom of Information Commissioner of Hungary plays an important role in defending the Hungarian citizens in the field of information security and violation of personal rights related to private information and data.

In the field of consumer protection, the National Communications Authority (*Nemzeti Hírközlési Hatóság*, the representative of the rights of consumers) has the duty to protect consumers and provide reliable information for consumers, including measures to be taken against computer-related crimes.

12.3.2 Contact details

Data Protection and Freedom of Information Commissioner
H-1015 Budapest, Nádor u. 22.
Phone: +36-1-475-71-86
Fax: +36-1-269-35-41
email: adatved@obh.hu
http://abiweb.obh.hu/dpc/index.htm

National Communications Authority of Hungary
H-1015 Budapest, Ostrom u. 23-25.
Phone: +36-1-457-7100
Fax: +36-1-356-5520
email: info@nhh.hu
http://www.nhh.hu/english/index1.html

12.3.3 Other reporting mechanisms

No major alternative reporting mechanisms.

12.4 Forensics

There is no pre-defined category of evidence that can be used in Hungarian criminal procedure. All kinds of evidence may be submitted. Electronic evidence is admitted as a common form of evidence. It is essential that the evidence has to be obtained in a lawful way.

When confronted with computer-related crime (through a complaint or discovery by the police), the police (Internet Screening Group) carry out a preliminary investigation, then the criminal investigation during which it obtains the evidence. The public prosecutor decides whether there is enough evidence for the impeachment. The public prosecutor may order additional inquiry or pass the procedure with impeachment to court. For certain coercive measures the permission of a judge is required. In some cases, a prosecutor or judge will use a civil expert to carry out the investigation. The suspect may also rely on an expert in case of a counter argument.

The following coercive measures may be available in computer related crime cases: search, seizure, preliminary sale and confiscation of seized property, reservation of computer-stored data, sequestration.

Under section 158/A of the Criminal Procedure Act, reservation of data means the temporary restriction of the right of disposal of a person possessing, processing or managing data recorded by a computer system (hereinafter: computer data) over specific computer data, in order to investigate and prove a criminal offence. The court, the prosecutor or the investigating authority orders the reservation of computer data constituting a means of evidence or required to trace any means of evidence or the establishment of the identity or location of a suspect. From the time of being notified of the order, the obliged party reserves the data recorded by the computer system designated in the order, and ensures its safe storage, if necessary, separately from other data files. The obliged party has to prevent the modification, deletion, destruction of the computer data, as well as the transmission and unauthorised copying thereof and unauthorised access thereto. The party ordering the reservation of data may affix its advanced electronic signature on the data to be reserved. While the measure is in effect, the data to be reserved may solely be accessed by the court, prosecutor or investigating authority having issued the order, and – with their respective permission – the person possessing or managing the data. The person possessing or managing the

data to be reserved may only provide information of such data with the express permission of the issuer of the order during the effect of the measure.

The obligation to preserve data may be in effect until the seizure of the data, but no longer than for three months. The obligation to reserve the data shall terminate if the criminal proceeding has been concluded. The obliged party shall be advised of the conclusion of the criminal proceeding.

12.4.1 **Data seizure**

The prosecutor may decide to make a copy of the hard disk to put it on a hard disk at the forensic workstation. If necessary, (part of) the access to the data and the copies thereof may be blocked or the data may even be deleted, e.g. because it is impossible to make a copy or in case of viruses. The prosecutor must inform the system administrator of the data that were copied, blocked or deleted and must guarantee the integrity and confidentiality of the seized data, e.g. through encryption and digital signature. Seized data are admissible as documentary evidence and supporting evidence. In the case of documentary evidence, they are backed up by other material evidence and declarations of the suspects and witnesses.

12.4.2 **Network searching**

The investigating authority may order a search of the network if deemed necessary to reveal the truth. There must be a risk that the data would otherwise get lost and the search may not go beyond the computer system or parts thereof to which the persons authorised to use the searched system have access. Data located on a computer system abroad may be copied but not blocked and the investigating magistrate must inform the ministry of justice who will notify the country in question.

12.4.3 **Involvement of experts**

The investigating authority may order persons who have the necessary expertise to provide information on the working of the relevant informatics system or on how to get access to the relevant electronic data. The network administrator may for instance be asked to provide a password or to provide information on the security technique adopted for the system. Anyone aware of these investigation measures, including the person requested to co-operate, is bound by a duty of confidentiality. Refusal to co-operate as well as breach of the confidentiality duty is subject to criminal sanctions.

The Hungarian State is liable for damage to the computer system or to the data as a result of these investigating measures.

12.5 References

- Criminal Code: Act No. IV. of 1978 ("Büntető Törvénykönyv")
- Act on the Criminal Procedure: Act No. XIX. of 1998 ("*a büntetőeljárásról szóló törvény*")
- Act no CXXI. of 2001 amending the Criminal Code introducing computer-related crime (*2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról*)
- Act no 63 of 1992 on the protection of personal data and publicity of data with public interest ("*A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény"*)
- Act no 108 of 2001 on the electronic commercial services and services related to information society ("*Az elektronikus kereskedelmi szolgáltatásokról és az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről"*)
- Act no 100 of 2003 on electronic communications ("*Elektronikus hírközlésről szóló törvény"*)

CHAPTER 13 Country report - Ireland

13.1 Irish legislation on computer crimes

Criminal Damage Act 1991 Sec. 5

Under Irish legislation, most of the computer crime related offences are handled by Sec.5 of the 1991 Criminal Damage Act. This section deals with unauthorized access and establishes that a person who, without lawful excuse, operates a computer within the State with intent to access any data kept either within or outside the State, or outside the State with intent to access any data kept within the State, whether or not he accesses any data, shall be guilty of an offence.

The penalty provided for this illicit conduct is a fine or a term of imprisonment not exceeding 3 months. This section applies also whether or not the person intends to access any particular data or any particular category of data or data kept by any particular person.

Criminal Justice (Theft and Fraud Offences Act) Act 2001 Section 9

A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years.

As can be seen this section is very broad and encompasses a broad list of offences.

Relevant Incidents	Applicable provision	Description	anction
Target Fingerprinting	Section 9 Criminal Justice (Theft and Fraud Offences Act) Act 2001.	A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.	A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years.
	Section 9 Criminal Justice (Theft and Fraud Offences Act) Act 2001.	A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.	A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years.
Malicious code	Criminal Damage Act 1991 Section 5: (1)	A person who without l\awful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) Outside the State with intent to access any data kept within the State, shall, whether or not be accesses any data, be guilty of an offence(2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person	A fine
Denial of service	Criminal Damage Act 1991 Section 5: (1)	A person who without l\awful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) Outside the State with intent to access any data kept within the State,	A fine

		shall, whether or not be accesses any data, be guilty of an offence(2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person	
Account compromise	Criminal Damage Act 1991 Section 5: (2) Subsection 1	(2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person	A term of imprisonment up to 3 months
Intrusion attempt	Criminal Damage Act 1991 Section 5	(1) A person who without l\awful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) (b) Outside the State with intent to access any data kept within the State, shall, whether or not be accesses any data, be guilty of an offence	A fine
		(2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person.	A term of imprisonment up to 3 months

Unauthorised access to information	Criminal Damage Act 1991 Section 5	(1) A person who without l\awful excuse operates a computer- (a) Within the State with intent to access any data kept either within or outside the State, or (b) Outside the State with intent to access any data kept within the State, shall, whether or not be accesses any data, be guilty of an offence	A fine
	Criminal Damage Act 1991 Section 5	(2) Subsection 1 applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person	A term of imprisonment up to 3 months
Unauthorised access to transmissions	European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003	Unsolicited direct marketing e-mail cannot be sent to individuals unless they have given their prior consent.	A person who fails to comply with these rules on direct marketing shall be guilty of an offence and liable to a fine of €3,000 in respect of each unsolicited telephone call, fax message, e-mail or SMS text.
Unauthorised modification of information	None as such	None as such	None as such
Unauthorised access to communication systems	None as such	None as such	None as such
Spam	None as such	None as such	None as such

13.2 Law enforcement bodies

13.2.1 Police (www.garda.ie/angarda/gbfi.html)

Ireland's National Police Service, Garda Siochana (Guardians of the Peace), is headed by a government appointed Commissioner. He is responsible to the Minister for Justice, Equality and Law Reform. The Commissioner's management team includes two Deputy Commissioners and 10 Assistant Commissioners. The Garda is responsible is responsible for all police functions in the state. It has some 11,230 personnel, including 1,700 non-uniformed detectives. Uniformed officers are unarmed, whereas detectives carry firearms.

13.2.2 Courts (www.attorneygeneral.ie)

Judges are appointed for life by the President on the advice of the government. District Courts which hears minor criminal and civil cases. More serious cases are heard by the Circuit Court. The High Court has full original jurisdiction and determining power in all matters of law or fact. It also hears appeals from the Circuit Court in civil cases. When hearing criminal appeals it is known as the Central Criminal Court. The Supreme Court is the court of final appeal.

13.3 Reporting

13.3.1 Competent authorities

The Garda Computer Crime Investigation Unit is located within the Garda Bureau of Fraud Investigation. It is a national reference centre for Law Enforcement requiring assistance in the investigation of computer related crime. The unit has expertise in forensic examination of computer hardware and storage devices. Interestingly, PABX fraud is highlighted specifically in the CCIU crime prevention advice. Garda Information Technology Division (the operational IT / IS support unit) also provides support to investigations in an operational capacity.

13.3.2 Contact details

Computer Crime Unit,
Garda Bureau of Fraud Section
Harcourt Square,
Harcourt Street
DUBIN 2
T: +353-1-6663708 / +353-1-6663746
F: +353-1-4752658
cciuhs@iol.ie

Office of the Data Protection Commissioner
3rd Floor,
Block 6
Life Centre
Abbey Street
DUBLIN 1
T: + 353 1 874 8544
F: + 353 1 874 5405
info@dataprotection.ie
http://www.dataprotection.ie

13.3.3 Other reporting mechanisms

The Internet Advisory Board (IAB) co-ordinates activities of the www.hotline.ie service, designed to fulfill reporting considerations for content related crimes. At a general level the IAB monitors illegal and harmful use of the Internet, but this is content related. It also tries to assist in self- regulation of the ISP industry in Ireland.

13.4 Forensics

No further details

13.5 References (www.irlgov.ie)

- Criminal Justice (Theft and Fraud Offences Act) Act 2001.
- Criminal Damage Act 1991 Sec. 5
- European Communities (Electornic Communications Networks and Services)(Data Protection and Privacy) Regulations 2003

CHAPTER 14 Country Report: Italy

14.1 Italian legislation on computer crimes

In the early nineties, the Italian Criminal Code was no longer considered sufficient to protect against new forms of crime caused by the increasing use of computer and communications technology.

Thus, computer crimes were introduced within the Criminal Code with by Act n°547 of 13 December 1993 concerning modification and integration of the Criminal Code and the Criminal Procedure Code involving cyber crime" (*Moficazioni ed Integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica)*. The legislator did not create a specific section in the Penal Code for new issues, as has happened in some European countries. Instead they were integrated using the old criteria. Computer system damages were incorporated near common damages, unauthorized access to computer or telecommunication systems near unauthorized access to private property, etcetera.

Other criminal provisions related to ICT were introduced by Act. n° 269 of 3 August 1998 regarding Child pornography (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitu), and Act. n° 438 of 15 December 2001 concerning conversion into Law, modifying D.L. n°364 of 18 October 2001, containing urgent provisions to combat international terrorism (Conversione in legge del 18 ottobre 2001, n°374, recante disposizioni urgenti per contrastare il terrorismo internazionale).

Last but not least is Legislative Decree n° 196 of 30 June 2003 that entered into force on January 1 2004, the so called "data protection code", also known as the "Privacy code". It does not specifically concern cyber-crime, but some of its provisions refer to the telecommunications field.

14.1.1 Specific legislation

In order to understand the provisions applicable to CSIRT's classification of incidents, it is necessary to describe what it is foreseen in the Criminal Code about cyber crimes:

article 615ter, quater and quinquies; article 617quater, quinquies and sexies; article 640ter; article 420, par.2 and 3; article 635bis; and the relevant provisions of the Privacy Code, article 167 and 130.

615 ter: Unauthorized access to a computer or telecommunications system

Anyone who, without authorisation, accesses a computer or telecommunication system protected by security measures, or maintains access to it against the expressed or implied will of the person who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.

The imprisonment ranges from one to five years:

1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices - even without a licence - the profession of a private investigator, or by abusing the capacity of a system operator.

2) if to commit the crime the culprit uses violence upon objects or people, or if he is clearly armed.

3) if the behaviour causes either the destruction of or damage to the system or the partial or total interruption of its functioning; or the destruction of or damage to the data, the information or the software contained in the system.

If the provisions of the 1st and 2nd paragraphs concern either military systems; or systems concerning public order, public security or civil protection (protezione civile) or any other system of public interest, the penalty is respectively one to five years or three to eight years' imprisonment. In the case described in the 1st paragraph, convictions are only possible after a complaint has been registered by the victim; the other cases can be prosecuted "ex-officio".

Article 615quater: Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems

Whoever illegally obtains, reproduces, distributes, transmits or delivers codes, key-words or any other means for accessing a computer or telecommunications system protected by safety measures in order to obtain a profit for himself or for another person or to cause damage to others, or whomever in any way provides information or instructions fit for the aforementioned purpose, is punished with imprisonment up to one year and a fine up to EUR 5.164,00.

The penalty is imprisonment from one until two years and a fine from EUR 5.164,00 to 10.329,00 in the case of one of the circumstances mentioned in paragraph 1, 2 or 4 of article 617quater (see above).

Article 615quinquies: Diffusion of a Computer Program Intended to Damage or to Interrupt a Computer System

Whoever distributes, transmits or delivers a computer program - created by himself or by another person – with the purpose to damage or indeed damaging a computer or telecommunication system, the data or the software contained on or relevant to it, or

which causes the partial or total interruption or an alteration in its functioning, is punished with imprisonment of up to two years and fined up to EUR 10.329,00.

- Article 617quater: Interception, impediment or illicit interruption of informatics or telematics communication

Whoever fraudulently intercepts, interrupts or stops communication concerning an informatics or telematics system or communication between one or more systems, is punished with imprisonment from 6 months to 4 years.

If the crime is considered an extremely serious offence, the same punishment will be applied to anyone who reveals the contents of the communication using any kind of public information system.

These crimes are only punished after the victim has registered a complaint.

§ 4 of this article specifies that prosecution ex-officio is allowed if the offence has been committed:

- by damaging an informatics or telematics system used by the State or any other organization related to it, or by any company providing public services or of public utility;
- by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service;
- by a person who practices - even without a licence - the profession of a private investigator.

In these cases, the punishment is increased to imprisonment between 1 to 5 years.

- Article 617quinqies: Installation of equipment for interception, interruption or impediment of informatics communication or telematics communication

Whoever installs equipment to intercept, prevent or interrupt informatics communication or telematics communication or communication between one or more systems without authorisation is punished by imprisonment from 1 to 4 years.

The penalty is imprisonment from 1 to 5 years in case of the circumstances described in article 617quater, paragraph 4.

- Article 617sexies: Falsification, alteration or deletion of the content of telecommunication

Whoever fraudulently creates, alters or deletes either entirely or in part any content that has been intercepted, even unintentionally, originating from a communications system related to a computer or a telecommunications system or between several such systems in order to obtain a profit for himself or for others or in order to cause damage to someone, is punished by imprisonment of 1 to 4 years, if the perpetrator makes use of the modified contents or lets anybody use it.

The penalty is imprisonment from 1 to 5 years in case of the circumstances described in article 617quater, paragraph 4.

- Article 640ter: Computer fraud

Whoever alters the functionality of a computer or telecommunications system in any way, or interferes without right in whatever way with data, information or software held in a computer or telecommunications system, in order to obtain a profit for himself or in order to cause damage to others, is punished by imprisonment of 6 months to 3 years and a fine of EUR 51,00 euro to 1.032,00.

If the crime is committed against a system belonging to the State or to any other organisation related to it, or by someone abusing his position as a system operator, the imprisonment can range between 1 to 5 years.

These crimes are only punished after the victim has registered a complaint.

- Article 420, §2 and 3: Damaging Public ICT Infrastructure

Attempting to damage or destroy ICT infrastructure of public interest or public databases or programs that have a public utility, is punished with imprisonment from 1 to 4 years. If this attempt results in actual damage to or destruction of such ICT infrastructure, public databases or programs or if their functioning is interrupted, the penalty is imprisonment from three to eight years.

- Article 635bis: Damaging Computer Systems

Whoever damages or destroys computer systems, software or data is punishable with a term of imprisonment ranging between six months and three years. If the crime is committed through abuse of power of a system administrator, the penalty ranges between one year and four years of imprisonment.

14.1.2 **Privacy Code**

The code is divided into three parts. The first part sets out the general data protection principles that apply to all organisations. Part two of the code provides additional measures that will need to be undertaken by organisations in certain areas, for example, healthcare, telecommunications, banking and finance, or human resources. Part three relates to sanctions and remedies. It is expected that the second part of the code will be developed further through the introduction of sectoral codes of practice.

Seven codes are planned (including surveillance, with particular regard to video surveillance, human resources, private investigators, and advertising/marketing) which will be developed in consultation with industry groups. The provisions relevant to us are in the second and third part, i.e. articles 167 and 130.

Article 167 is a general rule concerning sanctions foreseen for "unlawful data processing". Paragraph 1 establishes that "1. Any person who, with a view to obtaining a personal gain for himself or for another or with intent to cause harm to another, processes personal data in violation of Sections 18, 19, 23, 123, 126 and 130 or else of the provision made further to Section 129 shall be punished, if harm is caused, by imprisonment of six to eighteen months or, if the offence consists in data communication or dissemination, by imprisonment of six to twenty-four months, unless the activity can be qualified as a more serious offence.

Article 130 deals with unsolicited communications, and establishes as a principle that " 1. The use of automated calling systems without human intervention for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication shall only be allowed with the user's consent.

2. Paragraph 1 shall also apply to electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or any other means used for the purposes referred to herein."

Exceptions to this opt-in system can apply, e.g. when the services are similar to those that have been the subject of a sale and the data subject, after being adequately informed, does not object to this use, either initially or in connection with subsequent communications. The data subject must be informed of the possibility to object to the processing at any time,

The National Data Protection Commission *(Il Garante per la protezione dei dati personali)* can also choose to become involved in case of persistent breach of the provisions laid down in this Section. It may order the provider of electronic communications services, under Section 143(1), letter b), to implement filtering procedures or other practicable measures with regard to the electronic contact details for electronic mail used for sending the communications described above.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Article 615quater Criminal Code	Distribution, communication or provision to others of software produced with intent to cause damage, interruption or modification of a computer, telecommunication system or computer program	Imprisonment up to one year and a fine up to EUR 5.164,00.
			Imprisonment between one and two years and a fine between EUR 5.164,00 and 10.329,00 in case of aggravated circumstances (see above).
Malicious code	Article 420, § 2 and 3 Criminal Code	Damaging or destroying ICT infrastructure of public interest or public databases or programs that have a public utility; or interrupting their functioning	Imprisonment between three and eight years
	Article 615quinquies Criminal Code	Distributing, transmitting or delivering a computer program intended to damage or actually damaging to a computer or telecommunication system, the data or the software contained on it, or which partially or totally impedes its functioning	Imprisonment of up to two years and a fine of up to EUR 10.329,00
	Article 635bis Criminal Code	Destroying, damaging, or rendering partially or totally unusable: 1 – computer or telecommunication systems 2 – a computer program 3 – data	Imprisonment of 6 months to 3 years
			The maximum penalty is raised to 4 years if there are aggravating circumstances (see above)
	Article 640ter Criminal Code	Altering the functionality of a computer or telecommunications system in any way, or interferes without	Imprisonment of 6 months to 3 years and a fine of EUR 51,00 to 1.032,00

		right in whatever way with data, information or software held in a computer or telecommunications system, in order to obtain a profit for himself or in order to cause damage to others	The term of imprisonment ranges between 1 and 5 years if there are aggravating circumstances (see above).
Denial of service	Article 420, § 2 and 3 Criminal Code	Damaging or destroying ICT infrastructure of public interest or public databases or programs that have a public utility; or interrupting their functioning	Imprisonment between three and eight years
Account compromise	Article 615ter Criminal Code	Accesses a computer or telecommunication system protected by security measures without authorisation, or maintains access to it	Imprisonment of up to 3 years
			The term of imprisonment ranges between 3 and 8 years if there are aggravating circumstances (see above).
Intrusion attempt	Article 615ter Criminal Code	Accesses a computer or telecommunication system protected by security measures without authorisation, or maintains access to it	Imprisonment of up to 3 years
			The term of imprisonment ranges between 3 and 8 years if there are aggravating circumstances (see above).
Unauthorised access to information	Article 615quater Criminal Code	Distribution, communication or provision to others of software produced with intent to cause damage, interruption or modification of a computer, telecommunication system or computer program	Imprisonment up to one year and a fine up to EUR 5.164,00.
			Imprisonment between one and two years and a fine between EUR 5.164,00 and 10.329,00 in case of aggravated circumstances (see above).
	Article 615ter Criminal Code	Accessing a computer or telecommunication system protected by security measures	Imprisonment of up to 3 years

		without authorisation, or maintaining access to it	The term of imprisonment ranges between 3 and 8 years if there are aggravating circumstances (see above).
Unauthorised access to transmissions	Article 615quater Criminal Code	Distribution, communication or provision to others of software produced with intent to cause damage, interruption or modification of a computer, telecommunication system or computer program	Imprisonment up to one year and a fine up to EUR 5.164,00.
			Imprisonment between one and two years and a fine between EUR 5.164,00 and 10.329,00 in case of aggravated circumstances (see above).
	Article 617quater Criminal Code	Fraudulently intercepting, interrupting or stopping communication concerning an informatics or telematics system or communication between one or more systems	Imprisonment of 6 months to 4 years
			Imprisonment of 1 to 5 years in case of aggravated circumstances (see above).
	Article 617quinqies	Installing equipment intended to intercept or interrupt telecommunication without prior authorisation	Imprisonment from 1 to 4 years
			Imprisonment of 1 to 5 years in case of aggravated circumstances (see above).
	Article 617sexies	Fraudulently creating, altering or deleting either entirely or in part any content that has been intercepted and which originated from a communications system in order to obtain a profit for himself or for others, or in order to cause damage to someone if the perpetrator makes use of the modified contents or lets anybody use it.	Imprisonment from 1 to 4 years
			Imprisonment of 1 to 5 years in case of aggravated circumstances (see above).
Unauthorised modification of information	Article 615ter Criminal Code	Accessing a computer or telecommunication	Imprisonment of up to 3 years

		system protected by security measures without authorisation, or maintaining access to it	The term of imprisonment ranges between 3 and 8 years if there are aggravating circumstances (see above).
Unauthorised access to communication systems	Article 615ter Criminal Code	Accesses a computer or telecommunication system protected by security measures without authorisation, or maintains access to it	Imprisonment of up to 3 years
			The term of imprisonment ranges between 3 and 8 years if there are aggravating circumstances (see above).
Spam	Article 130 and 161 Privacy Code	The use of electronic communication (such as e-mail, MMS, SMS) for advertising purposes without the prior consent of the addressee; hiding the sender's identity or not providing a valid sender address	Imprisonment of six to twenty-four months, and/or a fine of up to EUR 54,000[21]

14.2 Law enforcement bodies

14.2.1 Police (www.poliziadistato.it)

In Italy ICT crime investigations are lead by three main law enforcement bodies: the State Police (*Polizia di Stato)*, the Carabinieri (*Arma dei Carabinieri)* and the Financial Guard (*Guardia di Finanza*).

Within the State Police there is a subsection dedicated to postal and communications crime (*Polizia Postale e delle Comunicazioni*), of which one particular section is devoted entirely to cyber crime investigation.

The *Carabinieri* have a subsection called the Carabinieri Scientific Investigations Group (*Raggruppamento Carabinieri Investigazioni Scientifiche (Ra.C.I.S)*), and its

[21] Article 161 of the Privacy Code allows fines when the data subject is not adequately informed regarding the purpose and extent of the data processing, amongst others. When sending spam, this provision will almost invariably apply. Article 161 allows fines of EUR 3,000 to 18,000. However, if sensitive or legal data are involved or the processing entails certain specific risks, or if more serious harm is caused to one or more data subjects, the fine is elevated to EUR 5,000 and 30,000. The amount can be tripled if it is found to be ineffective on account of the offender's economic status. Given that the additional circumstances of the second paragraph will rarely apply in the case of spam, the maximum amount specified in the table is EUR 18,000 x 3 = EUR 54,000.

Telematics Section (*Sezione Telematica*) is entrusted with high tech crime investigations.

The Financial Guard have the Special Technological Anti-Crime Cell (*Nucleo Speciale Anticrimine Tecnologico*).

14.2.2 Courts (www.cortedicassazione.it/)

Computer crimes, like any other common crimes, are judged by the Tribunal of First Instance (first court) and the Court of Appeal (appellate court). As a last possibly competent instance there is the Supreme Court (*Corte di Cassazione*), which rules only on points of law.

14.3 Reporting

14.3.1 Competent authorities

Computer crimes, like any other common crimes, need to be reported to the competent authority before being prosecuted. This competent authority is the Public Prosecutor (*Procura della Repubblica*). The Public Prosecutor directs investigations and delegates the competent police section to execute the necessary measures.

14.3.2 Contact details

Servizio Polizia Postale e delle
Comunicazioni Divisione Investigativa
Viale Europa N.175
Roma
T: +39 06 59588001 or
+39 3486080512
F: +39 06 59587817
E: polizia.comunicazioni@mininterno.it
W: www.poliziadistato.it/pds/
english/specialist.htm
Languages: Italian, English

National Privacy Protection Commission
(*Il Garante per la protezione dei dati personali*)
Piazza di Monte Citorio N. 121
00186 ROMA
T: +39 06.69677.1
F: +39 06.69677.785
E: garante@garanteprivacy.it
URL: ww.garanteprivacy.it
Languages: Italian

Nucleo Speciale Anticrimine Tecnologico
Via Marcello Boglione 84
00155 Roma
T.:+ 39 06 229381
W: www.gdf.it

Raggruppamento Carabinieri indagini Scientifiche
Viale di Tor di Quinto 151
00191 Roma
T.: +39 06 3331789
W.: www.carabinieri.it

14.3.3 Other reporting mechanisms

Particular organizations specialised in certain crimes have set up particular reporting mechanisms, e.g.:

- Child pornography: Telefono Arcobaleno (www.telefonoarcobaleno.com) and ECPAT Italia (www.ecpat.it), who can alert the police when they are informed of a child pornography crime that has been or is going to be committed. The Italian government has also invited the Internet Service Providers to create their own self-regulation codes and mechanisms to prevent such crimes.
- As more and more children were and still are surfing the internet, on 19th November 2003 the self-regulation Code "*Internet & Minori*" (Internet & Children) was defined.

  The Code is destined to be an important tool because it prevents the potential risks of destroying the social value of the Internet which could arise from the improper or harmful use of these technologies.

  Operators subscribing to the Code - who can be recognised through the Internet@Minori brand - are required to adhere to certain rules of conduct in the services they offer. Organisations that have subscribed to the Code are: AIIP (*Associazione Italiana Internet Providers*), ANFoV (*Associazione per la convergenza nei servizi di comunicazione*), Assoprovider (*Associazione Provider Indipendenti*), and Federcomin (*Federazione delle imprese delle Comunicazioni e dell 'informatica*)

  The code' s aims are:

  1. to help adults, children and families use the Internet in a responsible, informed manner that takes children's needs into account;
  2. to provide specific protection to prevent children from coming into contact with material which is illegal or harmful to their development;
  3. to offer children equal and safe access to Internet resources, in line with national and international legislation;
  4. to protect children's right to privacy and the correct use of their personal data;
  5. to ensure the full cooperation of the relevant authorities to prevent, counter and repress IT crime, particularly in the fight against the exploitation of children through prostitution, pornography, and sex tourism perpetrated through the Internet.

14.4 Forensics

Italian legislation does not have a specific forensic discipline concerning cyber crimes; instead, the general provisions of the Criminal Procedure Code (CPC) are applied. An exception is made by article 266bis CPC: interception of informatics and telematics communication; by article 14 Act n° 269 1998, which authorises the postal police to

create fake sites for the purposes of child pornography investigations; and by article 4 Act n° 438 2001.

Sections of the CPC which are applicable as mentioned above are: article 247 to 250 (searches), article 253 (seizure in general), and article 254 (seizure of correspondence).

There have been many court decisions on what can be seized. One of the most important is Sent Cass.Sez.III, n.1778/03, which established that the seizure can concern storage devices but may not include printers, scanners, or screens, which cannot be considered to be probative elements.

The police are charged with the preliminary investigation of alleged offences and the detection of their perpetrators, including the collection and holding of evidence. The defence counsel has the right to be present when the suspect is being questioned by the police. The police are obliged to report to the judicial authorities all offences involving ex officio prosecution which come to their attention.

Judicial proceedings begin with a preliminary judicial investigation.

In the case of flagrant offences, offences admitted by the suspect or offences demonstrated by clear evidence, the investigation is conducted by a magistrate of the public prosecutor's office (*istruzione sommaria*).

In all other cases, the investigation is carried out by an investigating judge (*istruzione formale*). It is the public prosecutor who decides which of the two procedures is to be followed, but a suspect may request that the investigating judge undertake the preliminary enquiry. If the suspect is in custody, the investigation must be carried out by the investigating judge if, after 40 days, the public prosecutor has not asked for discharge or trial.

During all phases of the judicial proceedings (pre-trial, trial and appeal), for the evaluation of evidence, the judge, the public prosecutor or the defence counsel may nominate an expert as foreseen by article 220 CPC.

The main problem about forensics which remains to be solved concerns the legal evaluation of digital evidence.

Another problem specific to internet crime in particular concerns the identification of the author of a specific crime. As in most countries, no satisfactory answer has been found to this question yet.

14.5 References

- Act n°547 of 13 December 1993 concerning modification and integration of the Criminal Code and the Criminal Procedure Code involving cyber crime (*Moficazioni ed Integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica)*

- Act. n° 269 of 3 august 1998 regarding Child pornography *(Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitu)*
- Act. n° 438 of 15 December 2001 concerning conversion into Law, modifying D.L. n°364 of 18 October 2001, containing urgent provisions to combat international terrorism (*Conversione in legge del 18 ottobre 2001, n°374, recante disposizioni urgenti per contrastare il terrorismo internazionale*)
- Sentenza Cassazione Sezione III n.1778/03
- P.Galdieri, Teoria e pratica nell'interpretazione del reato informatico, Giuffrè, Milano,
- G. Pica, Diritto penale delle tecnologie informatiche, Utet , Torino, 1999
- C. Pecorella, Il Diritto penale dell'informatica, Cedam, Padova, 2000
- G. Ilarda, G. Marullo (a cura di), Cybercrime: Conferenza internazionale- La Convenzione del Consiglio d'Europa sulla criminalità informatica, Giuffrè, Milano, 2004

14.5.1 **Particular cyber-crimes:**

- P. Galdieri, C.Giustozzi, M. Strano, Sicurezza e privacy in azienda, Apogeo, Milano, 2001
- M. Strano, B. Neigre, P.Galdieri, Cyberterrorismo, Jackson Libri, Milano, 2002

14.5.2 **Forensics:**

- G.Costabile, *Scena criminis, documento informatico e formazione della prova penale*, in www.altalex.com/index.php?idnot=7429
- D.Forte, *Le attività informatiche a supporto delle indagini giudiziarie*, in www.gdf.it/rivista2k/Rivista_2-2000/ARTICOLI/05_2-2000.htm
- L.Stilo, *Computer forensic. Il volto digitale della scena criminis.Necessità di protocolli omogenei,*www.crimine.info/pubblic/crimineinfo/articoli/computer.htm

CHAPTER 15 Country Report: Latvia

15.1 Latvian legislation on computer crimes

The Latvian Criminal Code was updated in 2002, introducing the following types of computer and network related crimes:

- Communication Interception
- Arbitrarily Accessing Computer Systems
- Unauthorized Acquisition of Computer Software
- Damaging of Computer Software
- Disseminating of Computer Viruses
- Violation of Safety Measures Regarding Information Systems

It has been debated among lawyers that the definition of terrorism under Latvian criminal law would also include cyber-terrorism. Due to the absence of suitable cases it is impossible to determine how courts would interpret that article.

Unfortunately the Code of Criminal Procedure currently in force has not defined any procedures or investigative measures specific to computer and network related crime; however the new Criminal Procedure Law which has been approved by parliament on 21 April 2005 and which will enter into force on 1 October 2005 has defined specific measures related to cyber-crime and network crime.

Where the applicable sanction is of a financial nature, it is measured in the minimum monthly wages. The value of a minimum monthly wage currently is 80 LVL (EUR 113.83).

The sanctions also occasionally refer to “custodial arrest”, as an alternative to imprisonment. In Latvian criminal law "custodial arrest" refers to a short term imprisonment from 3 days to six months[22].

22 Sections 38 and 39 of the Criminal Code explain this in greater detail:

Section 38. Deprivation of Liberty (described as “imprisonment” throughout this report – Ed.)

(1) Deprivation of liberty is the compulsory imprisonment of a person.

(2) Deprivation of liberty shall be determined for a term of not less than six months and not exceeding fifteen years, but for especially serious crimes – for a term not exceeding twenty years.

(3) In cases specifically provided for in this Law, deprivation of liberty may be determined for life (life sentence).

(4) The term of deprivation of liberty shall be determined in years and months, but in cases provided for in this Law, also in days.

Section 39. Custodial Arrest

(1) Custodial arrest is the holding of a person in short-term compulsory imprisonment.

(2) Custodial arrest shall be determined for a term of not less than three days and not exceeding six months. When substituting custodial arrest for a fine, a term not exceeding one year may be determined for such.

(3) During a term of custodial arrest, a person may be involved in performing indispensable public work, as determined by a local government.

(4) Soldiers shall serve their sentence in the guardhouse.

(5) Custodial arrest may not be applied to pregnant women and mothers caring for an infant not exceeding one year of age.

Relevant Incidents	Applicable Provision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime
Malicious code	Article 244 Criminal Code	Knowingly disseminating a computer virus, i.e. such means of programming as causes unsanctioned destruction or alteration of computer software or information, or damages information equipment, or destroys protection systems	Imprisonment of up to four years, or a fine of up to two hundred times the minimum monthly wage
		Committing the crime described above, causing substantial harm	Imprisonment of up to ten years.
Denial of service	Article 288 Criminal Code	Damaging through negligence telecommunications equipment, radio or television transmitters, or postal technology equipment, if this causes the interruption of related communications activities	Imprisonment of up to two years, or custodial arrest, or community service, or a fine of up to forty times the minimum monthly wage.
		Intentionally destroying or damaging telecommunications equipment, radio or television transmitters, or postal technology equipment.	Imprisonment between three and ten years.
	Article 243 Criminal Code	Modifying, altering, damaging or deleting, without authorisation, information stored in an automated computer-based system, or knowingly entering false information into an automated system, or knowingly damaging or destroying information bearing devices, computer software or protection systems, if substantial harm is caused thereby.	Imprisonment of up to five years, or a fine of up to one hundred and fifty times the minimum monthly wage.

Account compromise	Article 241 Criminal Code	Arbitrarily accessing an automated computer system, if this causes the opportunity for an outsider to acquire information entered into the system	Custodial arrest or a fine of up to eighty times the minimum monthly wage.
		Committing the crime above, by breaching computer software protection systems or accessing communications lines	Imprisonment of up to one year, or a fine of up to one hundred and fifty times the minimum monthly wage
Intrusion attempt	None as such	Only punishable as a preparatory act (attempt to commit another crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime
Unauthorised access to information	Article 144 Criminal Code	Intentional violation of the confidentiality of information, including through the use of programs provided for use in connection with electronic data processing	Community service, or a fine of up to five times the minimum monthly wage
		Committing the crime described above for the purposes of acquiring property	Imprisonment of up to three years, or custodial arrest, or community service, or a fine of up to sixty times the minimum monthly wage, with or without deprivation of the right to engage in specific activities for a period of up to five years.
	Article 241 Criminal Code	Arbitrarily accessing an automated computer system, if this causes the opportunity for an outsider to acquire information entered into the system	Custodial arrest or a fine of up to eighty times the minimum monthly wage.
		Committing the crime above, by breaching computer software protection systems or accessing communications lines	Imprisonment of up to one year, or a fine of up to one hundred and fifty times the minimum monthly wage
	Article 242 Criminal Code	Unauthorised copying of computer software, files or databases stored in the memory of a computer system, if this results in substantial harm.	Custodial arrest or a fine of up to eighty times the minimum monthly wage.
		Committing the crime above, by breaching computer software protection systems or accessing communications lines	Imprisonment of up to two years, or a fine of up to one hundred and fifty times the minimum monthly wage
Unauthorised access to transmissions	Article 144 sections 1 and 2 Criminal Code	Intentional violation of the confidentiality of personal correspondence or information in the form of transmissions over a telecommunications network.	Community service, or a fine of up to five times the minimum monthly wage

		Committing the crime described above for the purposes of acquiring property	Imprisonment of up to three years, or custodial arrest, or community service, or a fine of up to sixty times the minimum monthly wage, with or without deprivation of the right to engage in specific activities for a period of up to five years.
Unauthorised modification of information	Article 243 Criminal Code	Modifying, altering, damaging or deleting, without authorisation, information stored in an automated computer-based system, or knowingly entering false information into an automated system, or knowingly damaging or destroying information bearing devices, computer software or protection systems, if substantial harm is caused thereby.	Imprisonment of up to five years, or a fine of up to one hundred and fifty times the minimum monthly wage.
Unauthorised access to communication systems	Article 242 Criminal Code	Unauthorised copying of computer software, files or databases stored in the memory of a computer system, if this results in substantial harm.	Custodial arrest or a fine of up to eighty times the minimum monthly wage.
		Committing the crime above, by breaching computer software protection systems or accessing communications lines	Imprisonment of up to two years, or a fine of up to one hundred and fifty times the minimum monthly wage
Spam	Law on Information Society Services	Commercial messaging without previous acceptance from the receiving party as well as commercial messaging without an opportunity to unsubscribe from such messaging.	None

15.2 Law enforcement bodies

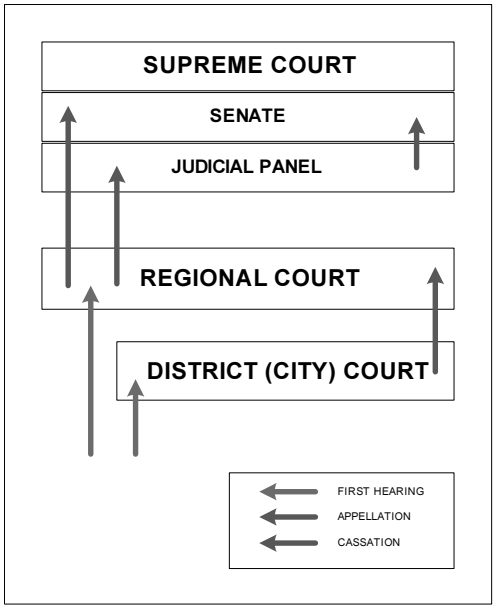
15.2.1 State Police (http://www.vp.gov.lv/)

The department of the State Police responsible for computer crimes is The Economic Police Department (*Ekonomikas policijas pārvalde* – EPD) which is under direction of the Central Criminal Police Department (*Galvenā kriminālpolicijas pārvalde*) .

15.2.2 Courts (http://www.tiesas.lv/eng/)

The court most likely to deal with computer crime is the Court of First Instance (District (City) Court or Regional Court), criminal matters section (*Rajonu (Pilsētu) Tiesas / Apgabaltiesa, Krimināllietu nodaļa*).

Against the decisions of the District (City) Court appeal can be logged with the Regional Court. Against the decisions of the Regional Court appeal can be logged in the Supreme Court / Criminal Matters Panel (*Augstākās Tiesas Krimināllietu Tiesas Palāta*). The Senate of The Supreme Court (*Augstākās tiesas senāts*) only hears points of law. The following image illustrates the hierarchy of Latvian court system and flow of the case between different bodies.



15.3 Reporting

15.3.1 Competent authorities

The Economic Police Department should be informed of any type of computer or network related crime.

15.3.2 Contact details

The Economic Police Department (*Ekonomikas policijas pārvalde)*
Stabu iela 89
LV-1050 Riga
Latvia
T: +371 7208663
E: epb@vp.gov.lv
URL:http://www.vp.gov.lv/structure/view.php?id=38
Languages: Latvian, English, German, Russian

National Privacy Protection Commission (*Datu Valsts Inspekcija*)
Kr.Barona 5-4
LV-1050 Riga
Latvia
T: +371 7223131
F: +371 7223556
E: info@dvi.gov.lv
URL: www.dvi.gov.lv
Languages: Latvian, English, German, Russian

15.3.3 Other reporting mechanisms

When a computer crime incident has an international nature, the originating law enforcement body should refer to *Interpol National Bureau* or *Europol National Bureau*.

Interpol National Bureau
Stabu iela 89
Riga
Latvia
T: +371 7208413
E: office@interpol.iem.gov.lv
URL:www.vp.gov.lv/structure/view.php?darb=99&id=110
Languages: Latvian, English, German, Russian

Currently there are no other legal bodies responsible for electronic crime prevention. However in the case of cyber attacks where the source can be identified, it is a commonly accepted practice to refer to responsible internet service provider via an email which address is of a following form: abuse@ispdomain. That is – if an attack would have originated from internet service provider "abcd.lv", the victim should send an email to abuse@abcd.lv . Though internet service providers carry no real law enforcement rights, this approach can be used to stop currently ongoing electronic attacks. The practice of maintaining and monitoring such email address has been accepted and is used by major internet service providers in Latvia. This approach can also be used in the case of spam.

15.4 Forensics

When confronted with computer crime (after a complaint or discovery by the police), the EPD will carry out the initial inquiry and forensics under the supervision of the public prosecutor. Upon receipt of the report from the EPD, the latter may order additional inquiry measures or pass the investigation on to an judge. For certain investigation measures such as searches, the judge has exclusive competence; however in the case of immediate need for the performance of the search, under certain conditions public prosecutor is allowed to make that decision on his own. In some cases, a prosecutor or judge will use a civil expert to carry out

the investigation. The suspect may also rely on an expert in case of a counter argument.

Evidence under Latvian criminal procedure is not regulated. All kinds of evidence may be submitted. Electronic evidence is admitted as a common form of evidence. The more authentic the evidence, the easier it will be to convince a judge during proceedings.

There are no specific computer crime investigation measures available under current Code of Criminal Procedure; however such measures and specific procedures will be available when new Criminal Process Law will come in force on 1st of October 2005.

15.5 References (www.likumi.lv;www.ttc.lv/?id=50)

- Criminal Law of 17th of June 1998
- Code of Criminal Procedure of 6th of January 1961
- Criminal Process Law of 21st of April 2005 / in force since 1st of October 2005
- Law of 4th of November 2004 concerning Information Society Services (*Informācijas sabiedrības pakalpojumu likums*)
- Law of 17th of November concerning electronic communications (*Elektronisko sakaru likums*)

CHAPTER 16 Country report - Lithuania

16.1 Lithuanian legislation on computer crimes

Lithuanian legislation does not provide for a specific law on cyber-crimes; however, several legal acts can be applied to computer crimes and offences. Computer crimes are criminalised by the new Criminal Code of the Republic of Lithuania (*Lietuvos Respublikos baudžiamasis kodeksas,* 2000) (hereafter referred to as "Criminal Code"), which includes certain crimes against informatics (destruction or modification of computer information, destruction or modification of computer programmes, appropriation and dissemination of computer information). Computer offences (e.g. spamming, unauthorized access to transmissions) are also penalized by the Administrative Code of the Republic of Lithuania (*Lietuvos Respublikos administracinių teisės pažeidimų kodeksas,* hereafter referred to as "Administrative Code").

In addition, specific legislation regulates separate aspects of computer related activities. For example, the Law on Copyright and Related Rights of the Republic of Lithuania (*Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas*) regulates the protection of computer programmes, databases and copyrights related thereto. The Law on Legal Protection of Personal Data of the Republic of Lithuania *(Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas)*, the Law on Electronic Communications of the Republic of Lithuania *(Lietuvos Respublikos elektroninių ryšių įstatymas)* and the Law on Advertising of the Republic of Lithuania *(Lietuvos Respublikos reklamos įstatymas) inter alia* prohibit spam and other forms of unsolicited communications.

The procedure of investigation of computer crimes is mainly governed by the Code of Criminal Procedure of the Republic of Lithuania (*Lietuvos Respublikos baudžiamojo proceso kodeksas,* hereafter referred to as "Criminal Procedure Code"). The procedure of investigation of certain other forms of computer misconduct and misuses is governed by the Administrative Code, the Law on Administrative Proceedings of the

Republic of Lithuania *(Lietuvos Respublikos administracinių bylų teisenos įstatymas)* and other legal acts.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	No special provisioning	May be regarded as an element of other crime	None as such.
Malicious code	Article 196 Criminal Code	Causing damage by erasing, destroying, eliminating or changing computer information or by using devices/computer programs with the aim to limit the use of such information	Public service, or a fine[23], or imprisonment of up to 3 years
	Article 197 Criminal Code	Causing damage by erasing, destroying, eliminating or changing a computer programme, or by disrupting or changing a computer network, or data, or a computer system	A fine, or imprisonment of up to 3 years (legal persons may be held liable as well)
	Article 153(1) part 1 Administrative Code	Damaging electronic communication or unauthorised access to an electronic communications network	A fine of LTL 250 to LTL 500 (approx. EUR 350 to 700). In case of repeated infractions the fine is increased to between LTL 500 and LTL 1000 (approx. EUR 700 to 1.400)
Denial of service	Article 197 Criminal Code	Causing damage by erasing, destroying, eliminating or changing a computer programme, or by disrupting the operation of a computer network, information system or data	A fine, or imprisonment of up to 3 years (legal persons may be held liable as well)
	Article 196 Criminal Code	Limiting the proper use of computer information by using devices/computer programmes	Public service, or a fine, or imprisonment of up to 3 years

[23] Fines for each incident are not specified in the applicable provisions of the Criminal Code, since the principle of individualised punishment is applied by the courts in each specific case. However, the general provisions of the Criminal Code provide for the minimal and maximal fines, which for the crimes in question vary from 1 MLS (Minimal Living Standard) to 100 MLS. In case of negligence fines can range from 1 MLS to 75 MLS; for legal persons they can go up to 10,000 MLS; the MLS at the moment equals LTL 125 (approx. EUR 180).

Account compromise	Article 198(1) Criminal Code	Unauthorised access and maintenance of access to a computer system or computer network by breaching security measures	Public service, or a fine, or taking into custody, or imprisonment of up to 1 year (legal persons may be held liable as well)
Intrusion attempt	Article 198(2) part 1 Criminal Code	Preparatory actions with a view of unauthorised access: producing, transferring, selling or other distribution of equipment or computer programmes that could be used for the intervention in private electronic communications or for gaining legally protected computer information about legal or natural persons, or for unauthorised access to a computer system, as well as passwords, access codes or other data of the kind, intending to commit a crime; or obtaining and detaining the above-mentioned equipment or programmes	Public service, or a fine, or taking into custody, or imprisonment of up to 1 year (legal persons may be held liable as well)
	Article 153(10) Administrative Code	Producing, keeping, using, importing, exporting, selling, leasing or otherwise distributing as well as modifying or installing decoding devices or programme equipment that can be used to access the protected services or other conditional access facilities (normally available for a certain fee).	A fine of LTL 1500 to LTL 3000 (approx. EUR 2.100 to 4.000) and confiscation of decoding devices or programme equipment of natural persons and representatives of companies, agencies and organisations, if their activities are not connected to electronic communications. In case of repeated infractions the fine is increased to between LTL 2000 and LTL 4000 (approx. EUR 2.800 to 5.600) and confiscation of decoders or other decoding devices or programme equipment
Unauthorised access to information	Article 198(1) Criminal Code	Unauthorised access and maintenance of access to a computer system or computer network by breaching security measures	Public service, or a fine, or taking into custody, or imprisonment of up to 1 year (legal persons may be held liable as well)

	Article 153(1) part 1 Administrative Code	Unauthorised access to an electronic communications network	A fine of LTL 250 to LTL 500 (approx. EUR 350 to 700). In case of repeated infractions the fine is raised to between LTL 500 and LTL 1000 (approx. EUR 700 to 1.400)
Unauthorised access to transmissions	Article 166 Criminal Code	Illegal interception of private communication (by mail or any other technical means)	Public service, or a fine, or freedom restraint[24], or taking into custody, or imprisonment of up to 2 years (legal persons may be held liable as well)
	Article 198(1) Criminal Code	Unauthorised access and maintenance of access to a computer system or computer network by breaching security measures	Public service, or a fine, or taking into custody, or imprisonment of up to 1 year
	Article 153(1) part 1 Administrative Code	Unauthorised access to an electronic communications network	A fine of LTL 250 to LTL 500 (approx. EUR 350 to 700). In case of repeated infractions the fine is increased to between LTL 500 and LTL 1000 (approx. EUR 350 to 700)
Unauthorised modification of information	Article 196 Criminal Code	Causing damage by erasing, destroying, eliminating or changing computer information or by using devices/computer programmes to limit the use of such information	Public service, or a fine, or imprisonment of up to 3 years
	Article 197 Criminal Code	Causing damage by erasing, destroying, eliminating or changing a computer programme, or by disrupting the operation of a computer network, information system or data	A fine, or imprisonment of up to 3 years (legal persons may be held liable as well)

[24] Freedom restraint is a criminal sanction, different from imprisonment. According to the Criminal Code, its duration varies from 3 months to 2 years. Persons convicted to freedom restraint may not change their place of residence without notifying the court or another competent institution. A court may also prohibit visiting certain places, meeting certain persons or groups of persons, or holding, using, purchasing, or possessing certain items. The court may oblige the culprit to be at home at a certain time, to reimburse fully or in part the damage caused or eliminate the damage by work, to start working or to register at labor exchange, to start studying, to perform public services for up to 200 hours during the period of freedom restriction, e.g. at health care centers or by taking care of invalids, the elderly etc., to start treatment from alcoholism, drug or toxic addiction, venereal disease (with the consent of the convicted person), etc.

Unauthorised access to communication systems	Article 197 Criminal Code	Causing damage by erasing, destroying, eliminating or changing a computer programme, or by disrupting the operation of a computer network, information system or data	A fine, or imprisonment of up to 3 years (legal persons may be held liable as well)
	Article 153(1) part 3 Administrative Code	Unauthorised connecting of terminal equipment resulting in the obstruction of electronic communications	A fine of LTL 250 to LTL 500 (approx. EUR 350 to 700). In case of repeated infractions the fine is increased to between LTL 500 and LTL 1000 (approx. EUR 700 to 1.400) and confiscation of the equipment used
	Article 153(1) part 1 Administrative Code	Damaging electronic communication or unauthorised access to an electronic communications network	A fine of LTL 250 to LTL 500 (approx. EUR 350 to 700). In case of repeated infractions the fine is increased to between LTL 500 and LTL 1000 (approx. EUR 700 to 1.400)
Spam	Article 214(23) Administrative Code	Use of electronic mail for advertising purposes without the prior, free, specific and informed consent of the addressee of the messages	A fine of LTL 500 to LTL 1000 (approx. EUR 700 to 1.400). In case of repeated infractions, the fine is increased to between LTL 1000 and LTL 2000 (approx. EUR 1.400 to 2.800).
	Article 22 part 6 Law on Advertising	Advertising by electronic mail supplied without consent or request of the recipient or in case the recipient clearly disagreed to receive advertising material	A fine of LTL 1000 to LTL 10.000 (approx. EUR 1.400 to 14.000) for operators of advertising activity (after they have been warned to stop the supply of advertising, but continue to do so)
	Article 189(14) Administrative Code	Refusal to follow the warning of the National Consumer Rights Protection Board to stop the supply of advertising in violation of the requirements of law	A fine of LTL 500 to LTL 1000 (approx. EUR700 to 1.400). In case of repeated infractions the fine is increased to between LTL 1000 and LTL 2000 (approx. EUR 1.400 en 2.800)

16.2 Law enforcement bodies

16.2.1 **Police (www.policija.lt)**

The Lithuanian police system consists of the Police Department under the Ministry of the Interior of the Republic of Lithuania, territorial police and specialized police bodies (e.g. Lithuanian Criminal Police Bureau, *Lietuvos kriminalinìs policijos biuras*), all engaged in community policing. Competent police units work together and with other law enforcement bodies during investigations. A special Cybercrime Unit ('cyberpolice') was established as part of the Crime Investigation Chief Board, Lithuanian Criminal Police Bureau as of October 1, 2001. The Cyberpolice is a unit of the central criminal police of the state, the mission of which is to ensure the enforcement of the provisions of the Convention on Cyber-Crime, to prevent, investigate and detect crimes that are being planned, are being committed and have been committed in cyber space.

16.2.2 **Courts (www.teismai.lt)**

Computer crimes are dealt with by district or regional courts depending on the severity of the crime. District courts (*apylinkiù teismai)* hear all criminal cases, except for those attributable to the jurisdiction of regional courts (*apygardù teismai)*. The latter are competent to hear cases where persons are accused of severe crimes (intentional crimes punishable by imprisonment for over 6 years) or if the accused are officials of government institutions (e.g. the members of parliament or government). Moreover, regional courts are entitled to hear any case that is within the jurisdiction of district courts of that region.

An appeal against decisions of district courts may be lodged with regional courts. When the regional courts themselves have acted as the courts of first instance the Lithuanian Court of Appeals (*Lietuvos apeliacinis teismas)* is the appellate instance. Lithuanian law also provides for a cassation of the decisions of the courts of both first instance and appellate instance. The Supreme Court of Lithuania (*Lietuvos Aukšèiausiasis Teismas)* is the only court hearing such cases, and will decide only on the merits of law.

16.2.3 **Other institutions**

Police and courts are the main law enforcement bodies; however, some other institutions have certain powers dealing with computer crimes and offences. Pre-trial investigations are carried out by pre-trial investigation officers, prosecutors or pre-trial investigation judges. The National Consumer Rights Protection Board (*Nacionalinì vartotojù teisiù apsaugos taryba prie Teisingumo Ministerijos)* may impose fines on legal and natural persons for spam. The State Data Protection Inspectorate (*Valstybinì*

duomenù apsaugos inspekcija) has the power to draw up reports of certain offences, e. g. related to illegal data processing. The Communication Regulatory Authority (*Lietuvos Respublikos ryšių reguliavimo tarnyba)* may impose fines for the infringement of conditions for the pursuit of electronic communications activities or the conditions of use of electronic communications resources.

16.3 Reporting

16.3.1 Competent authorities

The decree No. 290 of the Government of the Republic of Lithuania "On the control of the information not to be published on public networks and requirements for publishing of restricted public information" as of 5 March 2003 (*Lietuvos Respublikos Vyriausybės nutarimas ,,Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo,* hereafter referred to as the "Decree"), prepared in accordance with the Decision No. 276/1999/EC of the European Parliament and of the Council as of 25 January 1999 adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, provides legal definitions of information that may not be published on public networks (i.e. information defined as secret under Lithuanian legislation) and of restricted public information (i.e. content harmful to children), and also provides for a reporting mechanism. Restricted public information may only be published online following the requirements set by the Law on the Protection of Children from Negative Influence of Public Information (*Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas)* and the decree No. 681 of the Government of the Republic of Lithuania as of 2 June 2004, establishing specific means for marking of restricted content (*Lietuvos Respublikos Vyriausybės 2004 m. birželio 2 d. nutarimas Nr. 681)* (e.g. an obligatory introduction webpage as a warning about restricted content).

Violations of the Decree may be reported to the Police Department under the Ministry of Interior of the Republic of Lithuania by phone (+370 5 272 5372) or by email (informacija@policija.lt).

The Police Department, should violations of the Decree be identified (through a complaint or discovery by the police itself), will report to:

1. the Information Society Development Committee under the Government of the Republic of Lithuania (*Informacinìs visuomenìs plìtros komitetas prie Lietuvos Respublikos Vyriausybìs*);
2. the non-governmental Commission of Journalists' and Publishers' Ethics (*Žurnalistų ir leidìjù etikos komisija*, as well as the State Inspector of Journalists' Ethics (*Žurnalistų etikos inspektorius*) (provided violations were committed by electronic means of mass media (e.g. a news website, a website of a newspaper);
3. the hosts and other intermediary service providers in question;
4. the Lithuanian Criminal Police Bureau (which will in turn conduct its own investigation).

Other entities of operational activities are also empowered to conduct appropriate investigation, having informed the Police Department in advance. (e.g. criminal police, operational departments of the local police authorities; the full list of such entities is established by the decree No. 1559 of Government of the Republic of Lithuania as of 3 October 2002 (*Lietuvos Respublikos Vyriausybės 2002 m. spalio 3 d. nutarimas Nr. 1559)*, according to the Law on Operational Activities), upon receiving information on violations of the Decree.

A special website (http://www.ivpk.lt/filtrai/lt/, in Lithuanian only) of the Information Society Development Committee under the Government of the Republic of Lithuania provides news and general information on internet security, as well as a possibility for registered users to submit URLs of websites with suspected harmful content.

The Communications Regulatory Authority of the Republic of Lithuania also provides news and general information on internet security on its official website http://www.rrt.lt (information on internet security in Lithuanian only). However, no special reporting mechanism is established.

There are currently no special legal acts in the Republic of Lithuania with regards to reporting of violations not related to content. However, reports on any misuse of computers and network are in practice accepted by the following institutions through the phone numbers and email addresses for general contacts:

1. National Consumer Rights Protection Board under the Ministry of Justice of the Republic of Lithuania;
2. Information Society Development Committee under the Government of the Republic of Lithuania;
3. State Data Protection Inspectorate.

Criminal offences related to computers and network misuse may also be reported to local police authorities.

16.3.2 **Contact details**

Police Department under the Ministry of Interior Affairs of the Republic of Lithuania
Saltoniškių str. 19, LT-08105 Vilnius
T: +370 5 271 9731
F: +370 5 271 9978
E: informacija@policija.lt
URL: http://www.policija.lt
Languages: Lithuanian, Russian, English

Cybercrime Unit
Lithuanian Crimnial Polie Bureau
Chief Board of Crime Investigation
Saltoniškių str. 19, LT - 08105, Vilnius
Telephone: +370 5 271 7998; +370 5 271 7933;
Fax: +370 5 271 7997
E: cyberpolice@policija.lt
W: http://www.cyberpolice.lt

National Consumer Rights Protection Board under the Ministry of Justice of the Republic of Lithuania
Vilniaus str. 25, LT-01119 Vilnius
T: +370 5 262 67 51
F: +370 5 279 14 66
E: taryba@nvtat.lt
URL: http://www.nvtat.lt
Languages: Lithuanian, Russian, English

Information Society Development Committee under the Government of the Republic of Lithuania
Gedimino Ave. 56, LT-01110 Vilnius
T: +370 5 266 51 61
F: +370 5 266 51 80
E: info@ivpk.lt
URL: http://www.ivpk.lt
Languages: Lithuanian, Russian, English

State Data Protection Inspectorate
Gedimino Ave. 27/2, LT-01104 Vilnius
T: +370 5 279 14 45
F: +370 5 261 94 94
E: ada@ada.lt
URL: http://www.ada.lt
Languages: Lithuanian, Russian, English

16.3.3 **Other reporting mechanisms**

A special website (http://www.vaikaiirinternetas.net/, set up by a private entity; in Lithuanian only) provides information on the protection of children against any harmful influence of the Internet; however, no reporting mechanism is established.

By decree No. 315 of the Government of the Republic of Lithuania as of 24 March 2005 (*Lietuvos Respublikos Vyriausybės)*, a Computer Emergency Response Team (CERT) will be created under the Communications Regulatory Authority of the Republic of Lithuania by the end of the year 2006. Currently, a private "LITNET CERT" (website: http://cert.litnet.lt) is operating and accepting reports on computer security incidents by email (cert@litnet.lt), by phone (+370 37 300645) and by fax (+370 37 300643).

16.4 Forensics

Evidence in Lithuanian criminal procedure is regulated by the Criminal Procedure Code.

According to the provisions of the Criminal Procedure Code, the main actors of criminal investigation are the pre-trial investigation judge (who issues permits for important cases of investigation), prosecutor and pre-trial investigation officers.

Electronic evidence is classified by the Criminal Procedure Code as a standard type of document. The seizure of electronic evidence is not regulated by special legal provisions; therefore, general provisions on seizure apply. A permit of the pre-trial investigation judge is necessary for seizure. In urgent cases, the seizure may be ordered by decree of the prosecutor or a pre-trial investigation officer. The pre-trial investigation judge must give an *a posteriori* permit within 3 days following the seizure; if the permit is not issued, the evidence seized must be returned to its owners, while the collected information may not be considered as evidence in the later stages of criminal procedure.

During pre-trial investigations, the examination of evidence is conducted on the spot or elsewhere (e.g. if special equipment is required) by specialists (i.e. pre-trial investigation officers or other persons possessing necessary special knowledge).

Experts may be employed both during pre-trial investigations (by virtue of a ruling of the pre-trial investigation judge) and during court hearings (by virtue of a ruling of the judge) to provide an impartial finding in court on the matter being investigated, including computer-related crimes. The List of Forensic Experts of the Republic of Lithuania is compiled and managed by the Ministry of Justice of the Republic of Lithuania. Specialists not included in the List of Forensic Experts may only be employed if there are no listed experts with necessary qualification.

16.5 References (www.lrs.lt)

- Administrative Code of the Republic of Lithuania (1985) *(Lietuvos Respublikos administracinių teisės pažeidimų kodeksas)*
- Criminal Code of the Republic of Lithuania (2000) (*Lietuvos Respublikos baudžiamasis kodeksas*)

- Code of Criminal Procedure of the Republic of Lithuania (2002) *(Lietuvos Respublikos baudžiamojo proceso kodeksas)*
- Law on Administrative Proceedings of the Republic of Lithuania as of 14 January 1999 *(Lietuvos Respublikos administracinių bylų teisenos įstatymas)*
- Law on Legal Protection of Personal Data of the Republic of Lithuania as of 11 June 1996 *(Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas)*
- Law on Copyright and Related Rights of the Republic of Lithuania as of 18 May 1999 *(Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas)*
- Law on Electronic Communications of the Republic of Lithuania as of 15 April 2004 *(Lietuvos Respublikos elektroninių ryšių įstatymas)*
- Law on Advertising of the Republic of Lithuania as of 18 July 2000 *(Lietuvos Respublikos reklamos įstatymas)*
- Law on Protection of Children from Negative Influence of Public Information as of 10 September 2002 *(Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas)*
- Law on Operational Activities of the Republic of Lithuania as of 20 June 2002 *(Lietuvos Respublikos operatyvinės veiklos įstatymas)*
- Decree No. 290 of the Government of the Republic of Lithuania "On the control of the information not to be published on public networks and requirements for the publishing of restricted public information" as of 5 March 2003 *(Lietuvos Respublikos Vyriausybės nutarimas „Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo")*
- Decree No. 681 of the Government of the Republic of Lithuania as of 2 June 2004 *(Lietuvos Respublikos Vyriausybės 2004 m. birželio 2 d. nutarimas Nr. 681)*
- Decree No. 1559 of the Government of the Republic of Lithuania as of 3 October 2002 *(Lietuvos Respublikos Vyriausybės 2002 m. spalio 3 d. nutarimas Nr. 1559)*
- Decree No. 315 of the Government of the Republic of Lithuania as of 24 March 2005 *(Lietuvos Respublikos Vyriausybės 2005 m. kovo 24 d. nutarimas Nr. 315)*

CHAPTER 17 Country Report: Luxembourg

17.1 Luxembourg legislation on computer crimes

Most of the current cyber-crime provisions were introduced by the Law of 15 July 1993 combatting economical crime and IT fraud *(Loi tendant à renforcer la lutte contre la criminalité économique et la fraude informatique)*, and were incorporated in the Luxembourg Penal Code. The majority of the relevant provisions can be found in Title IX, Section VII of the second book of the Penal Code, entitled "Regarding certain ICT violations (*De certaines infractions en matière informatique)*, and in several provisions related to telecommunication protection. Available provisions focus mostly on unauthorized intrusions and damage resulting from such intrusions, ICT fraud, and the obstruction of the proper functioning of computer systems.

Relevant case law is largely unavailable, so that it is difficult to judge the efficiency of the current legislation.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another form of cyber-crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime
Malicious code	Article 509-2 Criminal Code	Intentionally and unlawfully hindering the proper functioning of an automatic data processing system	Imprisonment of 3 months to 3 years, and/or a fine of EUR 1.250 to 12.500
	Article 509-3 Criminal Code	Intentionally and unlawfully introducing, modifying or deleting data into an automatic processing system	Imprisonment of 3 months to 3 years, and/or a fine of EUR 1.250 to 12.500
Denial of service	Article 509-2 Criminal Code	Intentionally and unlawfully hindering the proper functioning of an automatic data processing system	Imprisonment of 3 months to 3 years, and/or a fine of EUR 1.250 to 12.500
	Article 509-3 Criminal Code	Intentionally and unlawfully introducing, modifying or deleting data into an automatic processing system	Imprisonment of 3 months to 3 years, and/or a fine of EUR 1.250 to 12.500
Account compromise	Article 509-1, section 1 Criminal Code	Fraudulently accessing or maintaining access to a data processing system.	Imprisonment of 2 months to 2 years and/or a fine of EUR 500 to 25.000
	Article 196 Criminal Code	Forgery of electronic credentials	Imprisonment of 5 to 10 years
	Article 488 Criminal Code	Fraudulently forging electronic keys	Imprisonment of 2 months to two years, and a fine of EUR 250 to 2.000
Intrusion attempt	Article 509-1, section 1 and 509-6 Criminal Code	Attempt to access a data processing system	Imprisonment of 2 months to 2 years and/or a fine of EUR 500 to 25.000
Unauthorised access to information	Article 509-1, section 1 Criminal Code	Fraudulently accessing or maintaining access to a data processing system.	Imprisonment of 2 months to 2 years and/or a fine of EUR 500 to 25.000
Unauthorised access to transmissions	Article 509-1, section 1 Criminal Code	Fraudulently accessing or maintaining access to a data processing system.	Imprisonment of 2 months to 2 years and/or a fine of EUR 500 to 25.000
	Article 2, sub 3 of the Privacy protection act	Voluntarily accessing the contents of a private message sent under closed envelope using whatever device, without the consent of the sender or the recipient	Imprisonment of 8 days to one year and/or a fine of EUR 62,5 to 1.250

	Article 3 of the Privacy protection act	Knowingly installing a device with the intention of accessing the contents of a private message without the consent of the sender or the recipient	Imprisonment of 8 days to one year and/or a fine of EUR 62,5 to 1.250
Unauthorised modification of information	Article 509-1, section 2 Criminal Code	Modifying or deleting data after fraudulently accessing a data processing system, or hindering its proper functioning	Imprisonment of 4 months to 2 years and/or a fine of EUR 1.250 to 25.000
Unauthorised access to communication systems	Article 509-1, section 1 Criminal Code	Fraudulently accessing or maintaining access to a data processing system.	Imprisonment of 2 months to 2 years and/or a fine of EUR 500 to 25.000
	Article 509-1, section 2 Criminal Code	Modifying or deleting data after fraudulently accessing a data processing system, or hindering its proper functioning	Imprisonment of 4 months to 2 years and/or a fine of EUR 1.250 to 25.000
Spam	Article 48 of the eCommerce Act	Sending out communications of a commercial nature without the prior consent of the recipient	Imprisonment of 8 days to one year and/or a fine of EUR 251 to 125.000

17.2 Law enforcement bodies

17.2.1 Police (www.police.public.lu)

The Police Corps and the Gendarmerie were amalgamated as of 1 January 2000 to form the Police Grand-Ducale, which carries out all police functions throughout the Grand Duchy. It is under the authority of the Ministry of the Interior, and contains a number of services, including the Judicial Police Service *(Service de Police judiciaire)*. This service is divided in a number of specialized sections, including the New Technologies section, which assists the investigating magistrate *(juge d'instruction)* in criminal investigations when required.

17.2.2 Courts

Criminal jurisdiction of Luxembourg has been attributed to four major courts: the Police Court (*Tribunal de Police*), the Criminal or Correctionnal Chamber of the Regional Court, (*Tribunal d'Arrondissement, Chambre criminelle/correctionnelle)*, the Criminal Chamber of the Court of Appeal (*Cour d'Appel, Chambre criminelle)* and the Supreme Court (*Cour de Cassation)*. The court most likely to deal with computer crime is the Criminal Chamber of the Regional Court.

Against its decisions, appeal can be lodged with the Court of Appeal (*Cour d'Appel*). The Supreme Court (*Cour de Cassation*) only hears points of law. Proceedings on the merits of

the case are always preceded by an inquiry under the supervision of the investigating magistrate *(juge d'instruction)*.

17.3 Reporting

17.3.1 Competent authorities

All incidents should be reported to the Police Grand-Ducale, who will involve the Judicial Police, section New Technologies when necessary. Additionally, the Luxembourg Ministry of Economy has recently established a new project, the Cyberworld Awareness Security Enhancement Structure (CASES). CASES functions similarly to many CERTs: it provides IT security information to the public, and contains a contact point where security threats may be reported.

17.3.2 Contact details

Judicial Police – New Technologies
Rue de Bitbourg 24
L-2957 Luxembourg
T : +35 2 4997 6410
F : +35 2 4997 6429
E: info@police.public.lu
URL: www.police.public.lu
Languages: German, French

National Privacy Protection Commission
(*Commission nationale pour la protection des données*)
Route de Luxembourg 68
L-4221 Esch-sur-Alzette
T: +35 26 1060 1
F: +35 26 1060 29
E: info@cnpd.lu
URL: www.cnpd.lu
Languages: French, German

17.3.3 Other reporting mechanisms

Apart from the Police Grand-Ducale, the main information security platform is the aforementioned CASES-project (www.cases.public.lu). The platform provides useful information regarding current security risks in Luxembourg, and allows visitors to report such risks. However, at the time of writing it does not specifically target the reporting of IT crimes, so that the Judicial Police remains the favoured contact point.

There is also a separate alert mechanism, where on-line child pornography reports can be filed. The site is hosted and managed by the Police Grand-Ducale, and can be found at http://www.police.public.lu/conseils_prevention/protection_enfance/preventionJeunesse/contact/index.php. Sites cannot be reported anonymously.

17.4 Forensics

Evidence in Luxembourg criminal procedure is not regulated. All kinds of evidence may be submitted, including electronic evidence. After an incident is reported, an investigating magistrate *(juge d'instruction)* will be appointed, who will lead the investigation, assisted by the judicial police.

No specific computer crime investigation measures have been introduced, although the law introducing the aforementioned criminal provisions also modified the Luxembourg Criminal Procedure Code. Article 7ter of this Code now specifies that a crime is considered to be committed on the territory of Luxembourg (and thus falls under its jurisdiction) when even one of its constituting elements was committed in Luxembourg. This doctrine allows extension of Luxembourg's legal authority beyond its physical borders.

For IT crimes, Luxembourg criminal procedure law relies heavily on interpretations of existing, more traditional provisions. Examples of potentially relevant provisions include sections of the Code regarding seizure (article 66 of the Criminal Procedure Code; traditionally only applied to documents and objects), searches (article 66) and telephone taps (article 88-1). The investigating magistrate can also order the participation of experts (article 87), and the suspect may choose to appoint an additional expert to assist in the investigation.

Due to a lack of suitable case law, it is difficult to assess whether the lack of IT crime specific provisions is a handicap in investigating IT incidents.

17.5 References (www.legilux.public.lu)

- Criminal Code (1879) and Criminal Procedure Code [1808]
- Law of 15 July 1993 combatting economical crime and IT fraud (*Loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique*)
- Law of 11 August 1982 regarding privacy protection *(Loi du 11 août 1982 concernant la protection de la vie privée)*
- Law of 14 August 2000 regarding eCommerce *(Loi du 14 août 2000 relative au commerce électronique)*

CHAPTER 18 Country report - Malta

18.1 Maltese legislation on computer crimes

Provisions of the Criminal Code and other acts are relied upon where traditional crimes have been committed by technological means involving computer systems. A number of specific acts of computer misuse per se have been criminalised under the Criminal Code in 2001 to deal with specific computer crimes (unlawful access to and use of, information, hardware misuse).

Provisions relating to computer crimes are also found in other laws, such as the Security Services Act, the Electronic Communications Act and the Electronic Commerce Act. Some offences are treated as administrative (e.g., spam) and administrative fines are envisaged for such offences.

With regard to searching and seizure, general rules of collecting, preserving and presenting evidence are used, supplemented by specific provisions in the Criminal Code, specifically stating that the police, in addition to its powers of the police to seize a computer machine, may require any information which is contained in a computer to be delivered to it in a form in which it can be taken away and in which it is visible and legible.

It is useful to note the following interpretation article (Article 337B Criminal Code) for the purposes of reading the table below:

- "computer" means an electronic device that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, software and communication facilities that are connected or related to a computer in a computer system or computer network;

- "computer network" means the interconnection of communication lines and circuits with a computer through a remote device or a complex consisting of two or more interconnected computers;
- "computer output" or "output " means a statement or a representation of data whether in written, printed, pictorial, screen display, photographic or other film, graphical, acoustic or other form produced by a computer;
- "computer software" or "software" means a computer program, procedure or associated documentation used in the operation of a computer system;
- "computer supplies" means punched cards, paper tape, magnetic tape, disk packs, diskettes, CD-roms, computer output, including paper and microform and any storage media, electronic or otherwise;
- “computer system” means a set of related computer equipment, hardware or software;
- "supporting documentation" means any documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data;
- a reference to a computer includes a reference to a computer network;
- a reference to data, software or supporting documentation held in a computer or computer system includes a reference to data, software or supporting documentation being transmitted through a computer network.
- a person uses software if the function he causes the computer to perform:

  (*a*) causes the software to be executed; or

  (*b*) is itself a function of the software.

- a reference to any software or data held in a computer includes a reference to any software or data held in any removable storage medium which is for the time being in the computer.

Relevant Incidents	Applicable provision	Description	anction
Target Fingerprinting	Article 337C(1)(f) Criminal Code	Without authorisation, taking possession of or making use of any data, software or supporting documentation	See Note 1 below the table
	Article 337F(4) Criminal Code	Producing any material or committing any other act preparatory to or in furtherance of the commission of any offence of unauthorised access.	The same punishment as provided for the relevant offence of unauthorised access.
Malicious code	Article 337C(1)(d) Criminal Code	Without authorization, preventing or hindering access to any data, software or supporting documentation.	See Note 1 below the table
	Article 337C(1)(e) Criminal Code	Without authorisation, impairing the operation of any system, software or the integrity or reliability of any data.	See Note 1 below the table
	Article 337C(1)(g) Criminal Code	Without authorisation, installing, moving, altering, erasing, destroying, varying or adding to any data, software or supporting documentation.	See Note 1 below the table
	Article 337D(b) Criminal Code	Without authorisation, taking possession of, damaging or destroying a computer, a computer system, computer network, or computer supplies used or intended to be used in a computer, computer system or computer network or impairing the operation of any of the aforesaid.	See Note 1 below the table
Denial of service	Article 337C(1)(d) Criminal Code	Without authorisation, preventing or hindering access to any data, software or supporting documentation.	See Note 1 below the table
	Article 337C(1)(e) Criminal Code	Without authorisation, impairing the operation of any system, software or the integrity or reliability of any data.	See Note 1 below the table

	Article 337D(b) Criminal Code	Without authorisation, taking possession of, damaging or destroying a computer, a computer system, computer network, or computer supplies used or intended to be used in a computer, computer system or computer network or impairing the operation of any of the aforesaid.	See Note 1 below the table
Account compromise	Article 337C(1)(a) Criminal Code	Without authorisation, using a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or using, copying or modifying any such data, software or support documentation.	See Note 1 below the table
	Article 337C(1)(f) Criminal Code	Without authorisation, taking possession of or making use of any data, software or supporting documentation.	See Note 1 below the table
	Article 337C(1)(i) Criminal Code	Without authorisation, using another person's access code, password, user name, electronic mail address or other means of access or identification information in a computer.	See Note 1 below the table
Intrusion attempt	Article 337F(4) Criminal Code	Producing any material or committing any other act preparatory to or in furtherance of the commission of any offence of unauthorised access.	The same punishment as provided for the relevant offence of unauthorised access.
Unauthorised access to information	Article 337C(1)(a) Criminal Code	Without authorisation, using a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or using, copying or modifying any such data, software or support documentation.	See Note 1 below the table

	Article 337C(1)(f) Criminal Code	Without authorisation, taking possession of or making use of any data, software or supporting documentation.	See Note 1 below the table
	Article 337C(1)(i) Criminal Code	Without authorisation, using another person's access code, password, user name, electronic mail address or other means of access or identification information in a computer.	See Note 1 below the table
	Article 15(1) Security Services Act	Intercepting a communication in the course of its transmission without a duly issued warrant or without having reasonable grounds to believe that person(s) by/to whom the communication is made/sent have consented to the interception.	Imprisonment of up to two years and/or a fine not exceeding MTL 5,000 (approx. EUR 11,500)
	Article 23(1) Electronic Commerce Act	Accessing, copying or otherwise obtaining possession of or recreating the signature creation device of another person without authorisation, for the purpose of creating, or allowing or causing another person to create an unauthorized electronic signature using such signature device.	See Note 2 below the table
	Article 23(5) Electronic Commerce Act	Accessing, altering, disclosing or using the signature creation device of a signature certification service provider used to issue certificates without authorization of the signature certification service provider, or in excess of lawful authorization, for the purpose of creating, or allowing or causing another person to create, an unauthorized electronic signature using such signature creation device.	See Note 2 below the table

Unauthorised access to transmissions	Article 15.(1) Security Services Act	Intercepting a communication in the course of its transmission without a duly issued warrant or without having reasonable grounds to believe that person(s) by/to whom the communication is made/sent have consented to the interception.	Imprisonment of up to two years and/or a fine not exceeding MTL 5,000 (approx. EUR 11,500)
	Article 16.(1)(a) Security Services Act	Intentionally disclosing by a person engaged in a wireless telegraphy or telecommunications service otherwise than in the course of his duty the contents of any communication which has been intercepted in the course of its transmission by means of that service.	Imprisonment of up to one year and/or a fine not exceeding MTL 5,000 (approx. EUR 11,500)

	Article 35.(3) Electronic Communi-cations Act	Committing of any of the following acts by any person employed or detailed for duty with or attached to an undertaking providing or authorised to provide electronic communications networks and/or services or associated facilities: giving any information with regard to any message with which he becomes acquainted by reason of his office to any person not entitled to receive such information; willfully altering or suppresses any message or the designation of the person to whom it is transmitted or to whom it is addressed, without a good cause; willfully omitting, delaying or obstructing the transmission or delivery of any message or canceling or destroying any message or an application for the transmission of any message without a good cause; willfully representing a message as having been sent by a person other than the sender or as being addressed to a person other than the addressee, or an application for the transmission of a message as having been made by a person other than the applicant, without good cause; willfully canceling or destroying any message not addressed to him or an application for the transmission of a message, without good cause; unlawfully withdrawing from the control of an undertaking, or of an individual employed or detailed for duty with, or attached to, an undertaking, a message addressed to another person.	Imprisonment of up to six months and/or a fine not exceeding MTL 10,000 (approx. EUR 23,000)

	Regulation 5(1) Processing of Personal Data (Electronic Communi-cations Sector) Regulations 2003	Listening, tapping, storing or undertaking any other form of interception or surveillance of communications and of any related traffic data by any person other than the user and without the consent of the user concerned.	An administrative fine not exceeding MTL 1,000 (approx. EUR 2,300)
Unauthorised modification of information	Article 337C.(1)(a) Criminal Code	Without authorisation, using, copying or modifying any data, software or supporting documentation.	See Note 1 below the table
	Article 337C.(1)(b) Criminal Code	Without authorisation, outputting any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever.	See Note 1 below the table
	Article 337C.(1)(c) Criminal Code	Without authorisation, copying any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held.	See Note 1 below the table
	Article 337C.(1)(f) Criminal Code	Without authorization, making use of any data, software or supporting documentation.	See Note 1 below the table
	Article 337C.(1)(g) Criminal Code	Without authorization, installing, moving, altering, erasing, destroying, varying or adding to any data, software or supporting documentation.	See Note 1 below the table
	Article 23(2) Electronic Commerce Act	Altering, disclosing or using the signature creation device of another person without authorisation, or in excess of lawful authorisation, for the purpose of creating or allowing or causing another person to create an unauthorised electronic signature using such signature creation device.	See Note 2 below the table

	Article 23(3) Electronic Commerce Act	Creating, publishing, altering or otherwise using a certificate or an electronic signature for any fraudulent or other unlawful purpose.	See Note 2 below the table
	Article 23(5) Electronic Commerce Act	Accessing, altering, disclosing or using the signature creation device of a signature certification service provider used to issue certificates without authorization of the signature certification service provider, or in excess of lawful authorization, for the purpose of creating, or allowing or causing another person to create, an unauthorized electronic signature using such signature creation device.	See Note 2 below the table
Unauthorised access to communication systems	Article 5.(1)(d) Electronic Communication Act	Using any electronic communications network or apparatus for a purpose other than that for which it was supplied or making improper use thereof.	A fine of up to MTL 10,000 (approx. EUR 23,000); in case of a continuing offence a further fine of up to MTL 2,000 (approx. EUR 4,500) for each day during which the offence continues.
	Article 337D.(a) Criminal Code	Without authorisation, modifying computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.	See Note 1 below the table
	Article 337C.(1)(i) Criminal Code	Without authorisation, using another person's access code, password, user name, electronic mail address or other means of access or identification information in a computer.	See Note 1 below the table
Spam	Regulation 10 Processing of Personal Data (Electronic Communications Sector)	Using any publicly available electronic communications service to make an unsolicited communications for the purpose of direct marketing by various means, including electronic mail, without prior explicit consent in writing to the receipt of such a communication	An administrative fine not exceeding MTL 1,000 (approx. EUR 2,300)

		by the person-recipient.	

Note 1: (Article 337F Criminal Code):

(1) Imprisonment for a term not exceeding four years and/or a fine not exceeding MTL 10,000 (approx. EUR 23,000).

(2) Where an offence constitutes an act which is in any way detrimental to any function or activity of Government, or hampers, impairs or interrupts in any manner whatsoever the provision of any public service or utility, whether or not such service or utility is provided or operated by any Government entity, the penalty shall be increased to imprisonment for a term from three months to ten years and/or fine of not less than MTL 100 (approx. EUR 230)and not exceeding MTL 50,000 (approx. EUR 116,000); provided that where a person is found guilty of an offence against this subarticle for a second or subsequent time, the minimum of the penalty for such an offence shall not be less than MTL 500 (approx. EUR 1,150).

(3) The penalties established under subarticle (2) shall also apply in the case of any relevant offence -

(a) where the offence is committed in any place by an employee to the prejudice of his employer or to the prejudice of a third party, if his capacity, real or fictitious, as employee, shall have afforded him facilities in the commission of the offence; and
(b) with the exception of subarticle (2), where the offence committed by a person is the second or subsequent offence.

Note 2: Article 24 Electronic Commerce Act:

Imprisonment of up to six months and/or a fine of up to MTL 100,000 (approx. EUR 232,000); and in the case of a continuous offence, a fine not exceeding MTL 1,000 (approx. EUR 2,300) for each day during which the offence continues.

Note 3: Article 337C.(4) Criminal Code:

Article 337C.(4) provides that:

- for the purposes of all offences of Article 337C(1), a person is deemed to have committed an offence irrespective of whether in the case of any modification, such modification is intended to be permanent or temporary;
- the form of any data output is immaterial;
- while for the purpose of establishing of whether a person has committed the offence of 'taking possession' under Article 337(1)(f), if such person has in his custody or under his control any data, software of supporting documentation which he is not authorized to have, he is deemed to have taken possession of it.

18.2 Law enforcement bodies

18.2.1 Police and Security Service (www.pulizija.gov.mt)

The Malta Police Force will investigate all crimes and reports relating to computer and network misuse, generally in the same manner as it will investigate all other crimes and contraventions.

The general public is encouraged to first make contact with their local police station, present in every village. Where the report or complaint relates to a crime proper which is merely aided by a computer, that is, not a cyber crime per se, the matter will be dealt with under general police competence. The report/complaint relating to cyber crime is then referred to the Cyber Crime Unit at Police General Head Quarters. The Cyber Crime Unit is a support service group working in conjunction with the other police departments and with international agencies, such as Interpol and Europol. In complex cases several other units such as the Vice Squad or Fraud Squad may work in conjunction with Cyber Crime Unit.

Security Service personnel have surveillance powers, but in practice this is function is currently limited. To this end a proposal has recently been tabled in favour of adopting a unified solution for interception by security services involving tracking, tracing, localisation, and eavesdropping through a common database working in conjunction with private sector entities. It is expected that this proposal will be given clearance in the near future.

18.2.2 Courts

Computer misuse is a crime regulated by Section 337B et seg. of the Maltese Criminal Code. As such the competent court is the Court of Magistrates as Court of Criminal Inquiry where proceedings are conducted under the authority of the inquiring magistrate, whose function it is to decide at the end of the proceedings whether or not to remit all documents and evidence to the Criminal Court for trial. This notwithstanding the accused may elect to be tried summarily, in which case the case will be heard by the Court of Magistrates as a Court of Criminal Judicature. The police have a duty to arraign before the court as soon as possible any person they suspect of having committed a crime. Appeal lies to the Court of Criminal Appeal.

18.3 Reporting

18.3.1 Competent authorities

Members of the general public are encouraged to report all cases of computer crime by filing a report at their local police station. Reports can also be lodged by email to computercrime@gov.mt or through the general Maltese police force web site (www.pulizija.gov.mt), where all submitted reports, even when anonymous, will be investigated. Reports can also be made directly to the Cyber Crime Unit on +35622942231/2.

At the local level the police station will inform Head Quarters and the report will be directed to the unit concerned. In cases of doubt involving computers the matter be also be referred to the Cyber Crime Unit which will investigate further. For example, in a case of paedophilia the matter may involve computer misuse and so the issue will be investigated by the Vice Squad and the Cyber Crime Unit working together.

18.3.2 Other reporting mechanisms

ISPs in Malta are obliged to promptly inform the competent public authorities of alleged illegal activity undertaken or information provided by the recipients of the ISP's services and to grant to such authorities upon request information enabling the identification of recipients of their services with whom they have storage agreements. Hosting providers are also obliged, on pain of being liable, upon obtaining knowledge or awareness of illegal activities, to expeditiously remove or disable access to the information in question.

ISPs also adhere to a Code of Practice, under which they must co-operate with the competent authorities regarding any request by the latter for co-operation or assistance

as entitled by law. In relation to illegal and harmful content, the Code of Practice prescribes ISPs:

1) to publish information about how customers may take adequate precautions to protect themselves from computer misuse and illegal and harmful content on the Internet;

2) to publish adequate warnings to customers on virus attacks and threats of a similar nature of which they are sufficiently aware;

3) to take such reasonable steps as are necessary to provide customers with information regarding supervision and control of minors' access to Internet content, and the procedures which customers may implement to control this.

The onus for implementing any such safeguards, however, rests solely with the customer.

18.4 Forensics

All evidence is admissible before the Court of Magistrates, although there is a duty to provide, as far as possible, the 'best evidence'. In terms of electronic evidence, the Electronic Commerce Act (Act III of 2001) has elevated electronic data to the level of admissible evidence.

With regard to the collection of evidence the police in line with their general duty to investigate all crimes and to collect evidence have the power to stop and search, the power to enter, search and seize and the power to seize and retain. In cases presided over by an inquiring magistrate the specific warrant is granted by the on-duty magistrate but in particular cases, such as where police intervention is required to prevent the commission of an offence or the suppression of evidence, the police can proceed without a warrant. So for example the police may investigate data logs with the power to enter and search the server.

In addition to their general power to seize and retain, the police in terms of Section 355Q of the Maltese Criminal Code may seize any computer while requesting that any information contained therein be delivered to them in visible and legible form.

Maltese legislation does not, however, currently provide for any data retention obligation. The Maltese police is currently working on a framework policy based on the EU proposals.

Moreover, in line with Malta's signing of the Cyber Crime Convention, the police have been given the power to issue a 'thaw and freeze' order against any individual, enjoining him/her to hold information until further notice.

The inquiring magistrate may also nominate any technical experts he/she deems necessary to assist in the investigation.

18.5 References (www.justice.gov.mt)

- Criminal Code (Chapter 9 of the Laws of Malta)
- Security Services Act (Act XVII of 1996, as amended), (Chapter 391)
- Electronic Communications (Regulation) Act (Act XXXIII of 1997, as amended), (Chapter 399)
- Electronic Commerce Act (Act III of 2001, as amended), (Chapter 426)
- Processing of Personal Data (Electronic Communications Sector) Regulations 2003, (Legal Notice 16 of 2003), under the Data Protection Act (Chapter 440)

CHAPTER 19 Country Report: The Netherlands

19.1 Dutch legislation on computer crimes

Most of the current cyber-crime provisions were introduced by the Computer Crime Act of 1993. All relevant material cyber-crime provisions have been incorporated in the second book of the Dutch Criminal Code. As such, they are all classified as crimes (*misdrijven*), as opposed to transgressions (*overtredingen,* in the third book of the Criminal Code). This is important, since according to Dutch criminal law, attempts and aiding and abetting are both only punishable where crimes are concerned.

For the most part, these crimes can be described as penetration of an automated device (art. 138a Criminal Code), disrupting the processing or functioning of an automated device (art. 161sexies and 161septies Criminal Code), altering data and rendering it unusable (art. 350a and 350b Criminal Code), and interception (139c, 139d and 139e Criminal Code).

Additionally, the Computer Crime Act modernized the Criminal Procedure Code, introducing e.g. network searches.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another form of cyber-crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime
Malicious code	Article 161sexies Criminal Code	Intentionally destroying, damaging or disrupting the processing or functioning of an automated device, or harming a safety measure implemented in said device	Dependent on the consequences. If none of the following consequences is present, the incident is not punishable. resulting in the unlawful impeding of the storage or processing of data intended for public services, or in the functioning of a public telecommunications service: imprisonment of up to six months, or a fine of up to EUR 45,000 resulting in the endangerment of goods or the provision of services: imprisonment of up to six years, or a fine of up to EUR 45,000 resulting in the endangerment of another person's life: Imprisonment of up to nine years, or a fine of up to EUR 45,000 resulting in the endangerment of another person's life, and the actual death of another person: Imprisonment of up to fifteen years, or a fine of up to EUR 45,000

	Article 161septies Criminal Code	Culpably destroying, damaging or disrupting the processing or functioning of an automated device, or harming a safety measure implemented in said device	Dependent on the consequences. If none of the following consequences is present, the incident is not punishable. resulting in the unlawful impeding of the storage or processing of data intended for public services, or in the functioning of a public telecommunications service; or in the endangerment of goods or the provision of services: imprisonment of up to three months, or a fine of up to EUR 11,250 resulting in the endangerment of another person's life: Imprisonment of up to six months, or a fine of up to EUR 11,250 resulting in the endangerment of another person's life, and the actual death of another person: Imprisonment of up to one year, or a fine of up to EUR 11,250
	Article 350a section 3) Criminal Code	Intentionally and unlawfully spreading or making available data intended to do harm by replicating itself within an automated device	Imprisonment of up to four years, or a fine of up to EUR 45,000
	Article 350a section 2) Criminal Code	Commiting the acts described in article 350a, section 1, using a publicly accessible telecommunications network and seriously damaging the data involved	Imprisonment of up to four years, or a fine of up to EUR 11,250
	Article 350a section 1) Criminal Code	Intentionally and unlawfully changing or deleting of data stored or processed on an automated device, or rendering such data unusable or inaccessible	Imprisonment of up to two years, or a fine of up to EUR 11,250

	Article 350b section 1) Criminal Code	Culpably causing the unlawful changing or deleting of data stored or processed on an automated device, or rendering such data unusable or inaccessible, if this causes serious damage to the data	Imprisonment of up to one month, or a fine of up to EUR 2,250
	Article 350b section 2) Criminal Code	Culpably causing the unlawful spreading or making available of data intended to do harm by replicating itself within an automated device	Imprisonment of up to one month, or a fine of up to EUR 2,250
Denial of service	Article 161sexies Criminal Code	Intentionally destroying, damaging or disrupting the processing or functioning of an automated device, or harming a safety measure implemented in said device,	Dependent on the consequences. If none of the following consequences is present, the incident is not punishable. resulting in the unlawful impeding of the storage or processing of data intended for public services, or in the functioning of a public telecommunications service: imprisonment of up to six months, or a fine of up to EUR 45,000 resulting in the endangerment of goods or the provision of services: imprisonment of up to six years, or a fine of up to EUR 45,000 resulting in the endangerment of another person's life: Imprisonment of up to nine years, or a fine of up to EUR 45,000 resulting in the endangerment of another person's life, and the actual death of another person: Imprisonment of up to fifteen years, or a fine of up to EUR 45,000

	Article 161septies Criminal Code	Culpably destroying, damaging or disrupting the processing or functioning of an automated device, or harming a safety measure implemented in said device	Dependent on the consequences. If none of the following consequences is present, the incident is not punishable. resulting in the unlawful impeding of the storage or processing of data intended for public services, or in the functioning of a public telecommunications service; or in the endangerment of goods or the provision of services: imprisonment of up to three months, or a fine of up to EUR 11,250 resulting in the endangerment of another person's life: Imprisonment of up to six months, or a fine of up to EUR 11,250 resulting in the endangerment of another person's life, and the actual death of another person: Imprisonment of up to one year, or a fine of up to EUR 11,250
	Article 350a section 2) Criminal Code	Committing the acts described in article 350a, section 1, using a publicly accessible telecommunications network and seriously damaging the data involved	Imprisonment of up to four years, or a fine of up to EUR 11,250
	Article 350a section 1) Criminal Code	Intentionally and unlawfully changing or deleting data stored or processed on an automated device, or rendering such data unusable or inaccessible	Imprisonment of up to two years, or a fine of up to EUR 11,250
	Article 350b section 1) Criminal Code	Culpably causing the unlawful changing or deleting of data stored or processed on an automated device, or rendering such data unusable or inaccessible, if this causes serious damage to the data	Imprisonment of up to one month, or a fine of up to EUR 2,250

Account compromise	Article 138a, section 1, sub a) Criminal Code	Penetrating an automated device intentionally and unlawfully, bypassing a certain security system	Imprisonment of up to six months, or a fine of up to EUR 4,500
	Article 138a, section 1, sub b) Criminal Code	Penetrating an automated device intentionally and unlawfully, using false keys, false signals or false identities	Imprisonment of up to six months, or a fine of up to EUR 4,500
Intrusion attempt	Article 138a, section 1, sub a) Criminal Code	Attempt to penetrate an automated device intentionally and unlawfully, bypassing a certain security system	Imprisonment of up to four months, or a fine of up to EUR 3,000
	Article 138a, section 1, sub b) Criminal Code	Attempt to penetrate an automated device intentionally and unlawfully, using false keys, false signals or false identities	Imprisonment of up to four months, or a fine of up to EUR 3,000
Unauthorised access to information	Article 138a, section 1, sub a) Criminal Code	Penetrating an automated device intentionally and unlawfully, bypassing a certain security system	Imprisonment of up to six months, or a fine of up to EUR 4,500
	Article 138a, section 1, sub b) Criminal Code	Penetrating an automated device intentionally and unlawfully, using false keys, false signals or false identities	Imprisonment of up to six months, or a fine of up to EUR 4,500
	Article 139c Criminal Code	Intentionally using a technical device to intercept or record data that were not intended for the perpetrator using a publicly accessible telecommunications network	Imprisonment of up to six months or a fine of up to EUR 11,250
Unauthorised access to transmissions	Article 139c Criminal Code	Intentionally using a technical device to intercept or record data that were not intended for the perpetrator using a publicly accessible telecommunications network	Imprisonment of up to six months or a fine of up to EUR 11,250
Unauthorised modification of information	Article 350a section 1) Criminal Code	Intentionally and unlawfully changing or deleting data stored or processed on an automated device, or rendering such data unusable or inaccessible	Imprisonment of up to two years, or a fine of up to EUR 11,250

	Article 350a section 2) Criminal Code	Committing the acts described in article 350a, section 1, using a publicly accessible telecommunications network and seriously damaging the data involved	Imprisonment of up to four years, or a fine of up to EUR 11,250
Unauthorised access to communication systems	Article 138a, section 1, sub a) Criminal Code	Penetrating an automated device intentionally and unlawfully, bypassing a certain security system	Imprisonment of up to six months, or a fine of up to EUR 4,500
	Article 138a, section 1, sub b) Criminal Code	Penetrating an automated device intentionally and unlawfully, using false keys, false signals or false identities	Imprisonment of up to six months, or a fine of up to EUR 4,500
	Article 139c Criminal Code	Intentionally using a technical device to intercept or record data that were not intended for the perpetrator using a publicly accessible telecommunications network	Imprisonment of up to six months or a fine of up to EUR 11,250
	Article 350a section 1) Criminal Code	Intentionally and unlawfully changing or deleting data stored or processed on an automated device, or rendering such data unusable or inaccessible	Imprisonment of up to two years, or a fine of up to EUR 11,250
	Article 350a section 2) Criminal Code	Committing the acts described in article 350a, section 1, using a publicly accessible telecommunications network and seriously damaging the data involved network.	Imprisonment of up to four years, or a fine of up to EUR 11,250
Spam	Article 11.7 section 1) Telecommunications Law	Using electronic messages for commercial, ideal or charitable purposes without the demonstrable prior consent of the recipient.	Administrative fine issued by OPTA after a complaint has been registered, of up to EUR 450,000 or 10% of the perpetrators turnover
	Article 11.7 section 3) Telecommunications Law	Using false identities in spam messages, or not including a valid return address for unsubscribe requests	Administrative fine issued by OPTA after a complaint has been registered, of up to EUR 450,000 or 10% of the perpetrators turnover

19.2 Law enforcement bodies

19.2.1 Police (www.politie.nl)

The Dutch police consists of 25 regional corps (*regionale korpsen*) and the National Police Service Corps (*Korps landelijke politiediensten (KLPD)*). The 25 regional corps are competent within their jurisdictions, while the KLPD organises national policing tasks.

Seven Digital Expertise Bureaus (*Bureaus Digitale Expertise*) are linked to the regions, with each Bureau providing assistance to one or more regions.

Finally, the Digital Investigations Group (*Groep Digitale Recherche*) is a subsection of the National Investigations Service (*Dienst Nationale Recherche)*. This Group conducts autonomous investigations, but can also be called upon to support the Digital Expertise Bureaus.

In addition, the Dutch government has founded a Computer Emergence Response Team (GOVCERT.NL), which acts as a central contact point for ICT crime incidents. Additionally, the centre provides information and support to private and public bodies.

19.2.2 Courts (www.rechtspraak.nl)

The court most likely to deal with computer crime is the general Court, criminal sector (*Rechtbank, sector strafrecht*). Against its decisions, appeal can be lodged with the Court of Appeal (*Gerechtshof*). The High Court (*Hoge Raad der Nederlanden*) only hears points of law. Proceedings on the merits of the case are always preceded by an inquiry under the supervision of the investigating magistrate.

19.3 Reporting

19.3.1 Competent authorities

GOVCERT.NL can be alerted in all cases of computer crime, such as denial of service attacks, hacking, fraud and any major computer crime incidents. They will offer any required assistance with the follow-up of security incidents.

The National Privacy Protection Commission (CBP) checks whether the collection of personal data is in line with the Law on Privacy Protection (WBP) and whether the information collected is needed for the purpose of the organisation that collects data.

19.3.2 Contact details

GOVCERT.NL
Nieuwe Duinweg 24-26
2587 AD The Hague
T : +31 70 888 78 5
F : +31 70 888 78 15
E: info@govcert.nl
URL: www.govcert.nl
Languages: Dutch, English

National Privacy Protection Commission
(*College Bescherming Persoonsgegevens*)
Post office box 93374
2509 AJ The Hague
T: +31 70 381 13 00
F: +31 70 381 13 01
E: info@cbpweb.nl
URL: www.cbpweb.nl
Languages: Dutch, English

19.3.3 **Other reporting mechanisms**

The most important initiative for securing information systems and networks is the Computer Emergency Response Team mentioned above (www.govcert.nl). GOVCERT.NL was established in June 2002 by the Dutch Government, with the purpose of preventing and dealing with ICT-related security incidents.

It acts as a central contact point for ICT-related security incidents, such as computer viruses, hacking and vulnerabilities in applications and hardware. Additionally, it offers assistance to public and private bodies in preventing security incidents and, if necessary, responding appropriately.

There are also several alert mechanisms for content related crimes, specifically concerning child pornography and discrimination.

- *Child pornography:* the private foundation "Meldpunt Kinderporno op Internet" (Reporting Point Child Pornography on the Internet) was founded in 1995, and provides an e-mail hotline for online child pornography (www.meldpunt.org). Reports can be sent to meldpunt@meldpunt.org, and will be treated anonymously. Reporters will receive a receipt confirmation and a sequence number, which can be used for further follow-up. The MKI will ensure that the report is passed on to the competent authorities, provided that the reported contents qualify as child pornography according to Dutch law.

- *Online discrimination:* a separate reporting mechanism exists for illegal forms of discrimination on the internet. The "Meldpunt Discriminatie Internet" (Reporting Point Discrimination Internet) was founded as a subsection of the private Magenta Foundation, and provides an e-mail hotline for online discrimination (www.meldpunt.nl). Users can report any allegedly unlawful expressions of discrimination based on religion, heritage, sexual preference, gender, race and/or age. The MDI will assess the complaints, and follow up on them, if they appear valid. Reports can be submitted to meldpunt@meldpunt.nl.

- Finally, spam can be reported with OPTA, the Dutch institution in charge of supervising the proper application of regulations regarding postal services and electronic communications. OPTA (www.opta.nl) has created a specific site to combat spam (www.spamklacht.nl), which contains all relevant information about Dutch spam regulations, and allows visitor to fill out an online complaint form (https://www.spamklacht.nl/asp/klachtindienen/) (page presently available in Dutch only). OPTA can sanction certain violations of Dutch anti-spam regulation with administrative fines of up to 450.000 Euros.

19.4 Forensics

Evidence in Dutch criminal procedure is not regulated. All kinds of evidence may be submitted, including electronic evidence.

Incidents can be reported to the district's officer of justice (*officier van justitie*), to any general investigating officer (*algemeen opsporingsambtenaar)* or a special investigating officer (*bijzonder opsporingsambtenaar*). Most commonly, the incidents are reported to the police, who qualify as general investigating officers. When specific support is required, they may request assistance from the Digital Expertise Bureaus or the Digital Investigations Group. These instances can then assist the police in the investigation, or continue it autonomously.

The following specific computer crime investigation measures are available:

19.4.1 Data seizure

There are currently no specific provisions on searching and seizing computer-related data. The traditional search provisions are considered to cover computer searches, and can be used to seize data-storage devices or to copy the information contained on them.

It is presently not possible to order persons under investigation to render data inaccessible, although the introduction of this measure is being considered as a part of the new Computer Crime II Bill.

19.4.2 Subscriber data

Public telecom service providers are required by law to retain certain telecommunications data. Article 13.4, section 2 of the Telecommunications Act obliges providers of mobile telecommunications to store the dates and times, cell phone call locations, and phone numbers of pre-paid card callers, for a period of three months. This obligation was created in order to enable the retrieval of identifying data of pre-paid card users.

For telecommunications data in general, art. 126na of the Criminal Procedure Code allows the investigation officer to oblige a public telecom provider to produce user data

(i.e., personal subscriber data or information regarding the provided service), if available.

19.4.3 Production orders

The investigating judge is allowed to order anyone with access to certain required data to produce this data, or to allow the judge to directly access the data (article 125i of the Criminal Procedure Code. To avoid self incrimination, the order cannot be given to a suspect. Additionally, there has to be a certain link between the data and the crime, the suspect, or logging data.

19.4.4 Network searching

Article 125j of the Criminal Procedure Code allows the extension of a local computer system search to other computers in a network, if these other computers are connected to the system that was originally being searched. However, this is only possible if the network is lawfully accessible to the people who regularly stay at the original search premises. Currently, a network search may not explore systems outside of the Dutch national borders.

19.5 References (www.wetten.nl)

- Criminal Code (1881) and Criminal Procedure Code [1921]
- Computer Crime Act of 1 March 1993 (*Wet computercriminaliteit*)
- Data Protection Act of 1 September 2001 (*Wet bescherming persoonsgegevens*)
- Telecommunications Act of 19 October 1998 (*Telecommunicatiewet*)

CHAPTER 20 Country Report: Poland

20.1 Polish legislation on computer crimes

Most of the typical computer misuse acts and computer security breaches have been labelled as offences in the Criminal Code of 6 June 1997. Procedural issues including search and seizures are regulated by provisions of the Criminal Procedure Code of 6 June 1997. Several amendments concerning computer crimes have since entered into force. The latest amendment of 18 March 2004 aimed to harmonise the Polish Criminal Code and the Criminal Procedure Code with the Council of Europe's Convention on Cybercrime.

Polish anti-spam regulation has been implemented by Parliament into the legal system through the Act of 18 July 2002 on electronically provided services. As a result, the distribution of unsolicited commercial information became a misdemeanour.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Generally-not penalized. Article 267 § 1 of the Criminal Code	Acquiring information without authorisation when that information was not intended for the interceptor by connecting to a wire that transmits information, or by breaching electronic, magnetic or other special protection	Imprisonment of 1 month to 2 years; restriction of liberty[25] from 1 to 12 months; and a fine from 10 to 360 day-fines (day-fine can be set from EUR 0,25 to EUR 500)
Malicious code	Article 269a of the Criminal Code	Unlawful hindering of the functioning of a computer system by transmitting, damaging, deleting, or altering computer data.	Imprisonment from 3 months to 5 years
	268a § 1 of the Criminal Code	Destroying, damaging, deleting or altering a record of essential information recorded on an electronic information carrier or otherwise obstructing or making it significantly more difficult for an authorised person to access it.	Imprisonment from 1 month to 2 years; restriction of liberty from 1 to 12 months; and a fine from 10 to 360 day-fines (day-fine can be set from EUR 0,25 to EUR 500)
	268a § 2 of Criminal Code	The crime described in article 268a § 1 is committed, resulting in significant material damages (ca. EUR 40.000 Euro or more)	Imprisonment from 3 months to 5 years
Denial of service	Article 269a of Criminal Code	Unlawful hindering of the functioning of a computer system by transmitting, damaging, deleting, or altering computer data.	Imprisonment from 3 months to 5 years
Account compromise	Article 269b § 1 of the Criminal Code	Unlawfully accessing an information system using hacking tools, or by unlawful possession of a computer password, access code, or similar data (even if no data is obtained)	Imprisonment between 1 month and 3 years

[25] The penalty of restriction of liberty is a kind of community-based sanction. While serving a restriction of liberty a convict may not change his permanent place of residence without the permission of the court. He is also obliged to perform 20-40 hours of work on a monthly basis for community benefit, and may be placed under supervision of a probation officer or another person of public trust. This penalty may be imposed for a duration ranging from 1 to 12 months.

Intrusion attempt	Articles 269b § 1 and 14 §1 of the Criminal Code	Attempting to unlawfully access an information system using hacking tools, or by unlawful possession of a computer password, access code, or similar data (even if no data is obtained)	Imprisonment between 1 month and 3 years
	Article 267 § 1 and 14 §1 of the Criminal Code	Attempting to acquire information without authorisation when that information was not intended for the interceptor by connecting to a wire that transmits information, or by breaching electronic, magnetic or other special protection	Imprisonment from 1 month to 2 years; restriction of liberty from 1 to 12 months; fine from 10 to 360 day-fines (day-fine can be set from Euro 0,25 to Euro 500)
Unauthorised access to information	Article 269b § 1 of the Criminal Code	Unlawfully accessing an information system using hacking tools, or by unlawful possession of a computer password, access code, or similar data (even if no data is obtained)	Imprisonment between 1 month and 3 years
	Article 267 § 1 of the Criminal Code	Acquiring information without authorisation when that information was not intended for the interceptor by connecting to a wire that transmits information, or by breaching electronic, magnetic or other special protection	Imprisonment of 1 month to 2 years; restriction of liberty from 1 to 12 months; and a fine from 10 to 360 day-fines (day-fine can be set from EUR 0,25 to EUR 500)
Unauthorised access to transmissions	Article 267 § 1 of the Criminal Code	Acquiring information without authorisation when that information was not intended for the interceptor by connecting to a wire that transmits information, or by breaching electronic, magnetic or other special protection	Imprisonment of 1 month to 2 years; restriction of liberty[26] from 1 to 12 months; and a fine from 10 to 360 day-fines (day-fine can be set from EUR 0,25 to EUR 500)

[26] The penalty of restriction of liberty is a kind of community-based sanction. While serving a restriction of liberty a convict may not change his permanent place of residence without the permission of the court. He is also obliged to perform 20-40 hours of work on a monthly basis for community benefit, and may be placed under supervision of a probation officer or another person of public trust. This penalty may be imposed for a duration ranging from 1 to 12 months.

	Article 269a of the Criminal Code	Unlawful hindering of the functioning of a computer system by transmitting, damaging, deleting, or altering computer data.	Imprisonment from 3 months to 5 years
Unauthorised modification of information	Article 269b § 1 of the Criminal Code	Unlawfully accessing an information system using hacking tools, or by unlawful possession of a computer password, access code, or similar data (even if no data is obtained)	Imprisonment between 1 month and 3 years
	Article 267 § 1 of the Criminal Code	Acquiring information without authorisation when that information was not intended for the interceptor by connecting to a wire that transmits information, or by breaching electronic, magnetic or other special protection	Imprisonment from 1 month to 2 years; restriction of liberty from 1 to 12 months; and a fine from 10 to 360 day-fines (day-fine can be set from Euro 0,25 to Euro 500)
Unauthorised access to communication systems	Article 269b § 1 of the Criminal Code	Unlawfully accessing an information system using hacking tools, or by unlawful possession of a computer password, access code, or similar data (even if no data is obtained)	Imprisonment between 1 month and 3 years
Spam	Article 24 Act of 18 July 2002 on electronically provided services	Distribution of unsolicited commercial information constitutes a misdemeanour.	Imprisonment for from 5 to 30 days, or restriction of liberty for 1 month, or a fine of up to PLN 5.000 (ca: EUR 1.250)

20.2 Law enforcement bodies

20.2.1 Police www.kgp.gov.pl

The organisational structure of the police has been regulated in the Police Act of April 6, 1990. The police is centrally organised and is governed by the Main Commander of Police, who is under supervision of the Minister of Interior.

The police force consists of six basic divisions: criminal police, traffic police, prevention and anti-terrorists squads, special police (e.g. for protection of railway and rivers), and local police. The Minister of Internal Affairs and Administration can establish other divisions if necessary. So far there is no separate computer crime division.

The logistic organisation of the police service in Poland reflects the administrative structure of the country. There is a Main Police Headquarters in Warsaw, and there are two lower levels of the police organisation operating throughout the country: provincial headquarters and regional headquarters. There is a Computer Crime Team located at the Main Police Headquarter in Warsaw. Its duty is to support police officers from all over the country in conducting computer related investigations. There are trained police officers specialising in fighting computer related crime in all provincial headquarters.

20.2.2 **Prosecution (www.ms.gov.pl/prokuratura)**

Prosecution in Poland is hierarchically organised. The Minister of Justice also holds the office of Attorney General, and he is in charge of all operations concerning prosecution. The Attorney General issues binding guidelines and instructions upon the public prosecutors. He may undertake all acts within the scope of operation of the Prosecution Service, and he can usually order his subordinate prosecutors to act on his behalf. He may also take over activities of his subordinate prosecutors when he feels it necessary.

The Prosecution Service consists of the following units: the National Prosecutor's office within the Ministry of Justice, the appellate units, provincial units and district units.

The prosecutors operate according to the principle of a hierarchical subordination, which means that they follow the regulations, guidelines and instructions of their superiors. However, they are independent in exercising their statutory duties. Their responsibility is to guard the observance of the rule of law and to enforce prosecution of crimes. Public prosecutors conduct preparatory proceedings in criminal cases and supervise investigations carried out by the police. They also act as attorneys for the state during criminal cases. The structure and functioning of prosecution in Poland is regulated by the Prosecution Service Act of 20 June 1985.

A distinguishing feature of prosecution in Poland is so called "legalism rule". According to this rule a prosecutor has no discretionary powers regarding the decision to prosecute: he must prosecute every detected crime.

20.2.3 **Courts www.ms.gov.pl/sady**

The most important jurisdiction in terms of criminal caseload is that of the District Courts (*Sądy Rejonowe*), which is competent for both civil and criminal matters. There are 310 District Courts. District court judges hear criminal cases concerning most offences and misdemeanors, excluding the most serious felonies. Almost all computer related crimes defined in the Criminal Code fall under the competence of District Courts. The only exception is so called "computer espionage". This crime entails the illegal collection of computer data related to national security, with the criminal intention of passing it on to foreign intelligence.

An appeal against a decision from a District Court will proceed directly to an appellate division of a Circuit Court (*Sąd Okręgowy*). There are 44 Circuit Courts. Circuit Courts also have a general jurisdiction as first instance courts for more significant criminal cases (including computer espionage), in addition to their appellate function. When cases are heard by a Circuit Court in first instance, parties may lodge an appeal with an Appellate Court (*Sąd Apelacyjny*). There are 10 Appellate Courts in Poland.

The judges in Poland are independent and subject only to the law. They are appointed for life and can not be dismissed, except by a decision of the National Council of Judiciary. The organisation and operation of the Polish courts is regulated by the Common Court System Act of 27 July 2001.

20.3 Reporting

20.3.1 Competent authorities

The competent authorities to be informed about any crime in order to prosecute are the police and the public prosecutor. Polish criminal procedure provides two methods for initiating criminal proceedings. The first is a crime report originating from a victim or witness, which must be submitted in a written form or in the form of an oral testimony. The second method consists of the prosecution acting *ex officio* whenever the police or public prosecutor obtains indicative information that a crime has been committed.

There are no separate reporting authorities with regard to computer related crimes. Therefore, a written or oral report on such a crime can be filed with any police station or any prosecutor's office in the country. An electronically filed form is thus far inadmissible. However, even a message sent by e-mail or fax can be enough to start proceedings *ex officio,* on the condition that it contains convincing indications that a crime has been committed. Therefore, it is possible to electronically notify the Computer Crime Team located at the Main Police Headquarters.

20.3.2 Contact details

There is a police hotline that can be used to file reports with the Polish Main Police Headquarters: +48 800 120 226. The Computer Crime Team of the Main Police Headquarter in Warsaw can also be contacted directly through hajduk@kgp.gov.pl

Further contact information for provincial police headquarters can be found at: http://www.kgp.gov.pl/komend.html

Contact information for all prosecutor offices in Poland can be found at: http://www.ms.gov.pl/organizacja/adresy_prok.doc

The Polish data protection bureau (*Biuro Generalnego Inspektora Ochrony Danych Osobowych, GIODO*) has its own Polish language website (www.giodo.gov.pl); a limited English and French translation is also available.

The bureau can be contacted directly at the following coordinates:

Biuro Generalnego Inspektora Ochrony Danych Osobowyc
ul. Stawki 2
00-193 Warszawa
Polska

T: +48 (22) 860-70-86
E: kancelaria@giodo.gov.pl

20.3.3 **Other reporting mechanisms**

The most widely recognised non-governmental initiative for securing information systems is the Computer Emergency Response Team Polska (CERT Polska). It was originally established under the name CERT NASK in March 1996 by the NASK (Research and Academic Network in Poland). Since February 1997, CERT POLSKA has been a full member of the worldwide Forum of Incident Response and Security Teams. Despite its name change, the team still consists of employees of the NASK, supported by experts from Polish universities.

CERT Polska's goals are:

- To provide a single, trusted point of contact in Poland for computer networks in Poland to deal with network security incidents and their prevention
- To respond to security incidents in networks connected to NASK and networks connected to other Polish Internet providers
- To report security incidents, thus providing security information and warnings of possible attacks in cooperation with other incident response teams all over the world

CERT Polska can be reached by phone (+48 22 5231274,) fax (+48 22 5231399), e-mail (cert@cert.pl) or WWW (http://www.cert.pl/)

Apart from CERT Polska, there is also a well known non-governmental initiative for tracing and reporting child pornography on the Internet, run by the Foundation Kidprotect. The aim of the foundation is to prevent the use of new media for the dissemination of child pornography, to protect children against sexual abuse and to provide a help-line for those in need. Kidprotect's volunteers specialize in collecting and verifying information about illicit content on the Web and cooperate closely with the police. Reports can be filed by phone (48 693 254 898), or by e-mail: hotline@kidprotect.pl

20.4 Evidence

Generally, there are no exclusion rules that would concern electronic evidence. All kinds of evidence are admissible, upon the judge's discretion. The only requirement is that the evidence must be presented in a form that is readable to the human senses. Therefore, the form and method of presentation of electronic evidence is largely unregulated in criminal procedure. On some occasions the assessment of evidence can be done with the help of a court-appointed expert or specialist. Usually, this would be done by a skilled network administrator or computer programmer presenting testimony (so called "opinion") during court trial.

There are some specific provisions concerning search and seizure of stored data that generally reflect solutions adapted in the Council of Europe's Convention on Cybercrime. These provisions mostly concern disclosure, production and preservation of traffic and billing data.

During the course of criminal proceedings, the police, prosecutor and court may order a telecommunication service provider to disclose and to produce data that have been already stored in service providers' computer systems, i.e. traffic and billing data (Article 218 §1 of the Criminal Procedure Code, and article 20c 1 of the Police Act).

The prosecutor and the court may also order the immediate preservation and collection of specific traffic and billing data for a period of up to 90 days, which can subsequently be extended (Article 218a § 1 of the Criminal Procedure Code). So far the police is however not equipped with instruments enabling the preservation of computer data (neither stored data, nor for data to be collected).

With regard to search and seizures of electronic evidence all the rules set in the Criminal Procedure Code for collection and presentation of traditional evidence should be observed (Article 236a of the Criminal Procedure Code). The police must obtain a warrant issued by a court or public prosecutor in order to search premises and persons. In case of emergency (where there is a risk of losing evidence and a warrant cannot be issued in advance) the search may be performed without a warrant. Such a warrantless search must be acknowledged and approved by the prosecutor or by the court within 7 days. The same rules apply to search and seizures of computer data, computers and computer systems.

The real time interception of electronic communications is allowed only in case of criminal investigation and for the prevention of the most serious crimes. These crimes are enumerated in the provisions of Article 237 § 3 of the Criminal Procedure Code and in Article 19.1 of the Police Act. Computer related offences usually do not fall into this category; however on some occasions these offences can be a preparatory step for committing crimes which do allow real time interception. Such interceptions can be ordered by a court or by a prosecutor.

20.5 References

- Criminal Code of 6 June 1997
- http://www.rzeczpospolita.pl/prawo/doc/kkarny2005/spis_tresci.html
- Criminal Procedure Code of 6 June 1997 http://www.rzeczpospolita.pl/prawo/doc/Kpk/Kpk_spis.html
- Act of 18 July 2002 on providing services in electronic way
- Police Act of April 6, 1990 http://www.kgp.gov.pl/prawo/ustawa.htm
- Prosecution Service Act of 20 June 1985 http://www.ms.gov.pl/organizacja/ust_prok.doc
- Common Court System Act of 27 July 2001 http://www.ms.gov.pl/organizacja/usp.doc

CHAPTER 21 Country report - Portugal

21.1 Portuguese legislation on computer related crimes

Portugal has a long tradition in the enactment of computer crime protection. In fact, Portugal has had a legal framework to be applied to criminal actions involving computers since 1991 (Law 109/91, of 17 August 1991) (Computer Crime Law - *Lei da Criminalidade Informática*).

The referred act follows the minimal list of Recommendation (89)9 of the European Council.

In 1998, a new computer crime was added: computer-related fraud. As the scope of protection is mainly the property, the Portuguese legislator considered that this crime should be included in the Criminal Code (and not in the Law 109/91), which leads to an unjustifiable lapse: in this case, companies will not be subject criminal liability (which happens in the event of condemnations under the Computer Crime Law).

Furthermore, Law 67/98, of 26 October 1998 (Personal Data Protection Law - *Lei de Protecção de Dados Pessoais*) should also apply in cases where there is an unauthorised access to personal data.

In addition, Portugal has transposed Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 in two different laws: Decree-Law n.º 7/2004 of 7 January 2004 (the e-Commerce Law - *Lei do Comércio Electrónico*) and Law no. 41/2004, of 18 August 2004.

Under these acts, Portugal adopted a provision imposing data retention obligations on operators and service providers of electronic communication (Law no. 41/2004, of 18

August 2004) and also a specific legal framework in relation to anti-spamming acts (punished by administrative sanctions).

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Article 8 of Law 109/91	Intercepting a communication process within a system without authorisation using technical devices	Imprisonment of up to 3 years or a fine[27] Attempt shall also be punishable
Malicious code	Depending on object of the action and on the intention of the agent: Article 5 of Law 109/91 or	Intentionally causing damage through the total or partial suppression or deletion of data or a computer programme, in order to gain an illegitimate benefit for the agent or for a third party.	Imprisonment of up to 3 years or a fine If the damage ranges between EUR 4,450 and EUR 17,799, the penalty is up to 5 years of imprisonment If the damage is EUR 17,800 or more, the penalty is from 1 year of imprisonment up to 10 years of imprisonment Attempt shall also be punishable
	Article 6 of Law 109/91	Introducing, modifying, erasing, or suppressing data or computer programmes or by other means intervening in a system, with intent to impede or disturb the functioning of a computer system or a distance communication data system	Imprisonment of up to 3 years or a fine of up to 600 days If the damage ranges between EUR 4,450 and EUR 17,799, the penalty is from 1 year of imprisonment up to 5 years of imprisonment For these penalties, procedures are dependent upon a prior complaint. If the damage is EUR 17,800 or more, the penalty is from 1 year of imprisonment up to 10 years of imprisonment
Denial of service	Article 6 of Law 109/91	Introducing, modifying, erasing, or suppressing data or computer programmes or by other means intervening in a system, with intent to impede or disturb the functioning of a computer system or a distance communication data system	Imprisonment of up to 3 years or a fine of up to 600 days If the damage ranges between EUR 4,450 and EUR 17,799, the penalty is from 1 year of imprisonment up to 5 years of imprisonment If the damage is EUR 17,800 or more, the penalty is from 1 year of imprisonment up to 10 years of imprisonment

[27] In relation to fines, Portuguese criminal law can autonomously define a time frame (e.g. from x to y days). In such cases, the limit is a minimum of 10 days and maximum of 360 days. For each day a fine amount will be fixed; if nothing is said to the contrary, the range is from EUR 1 to EUR 499. The number of days and the amount per day is decided by the judge (who decides under general and discretionary rules such as the guilt, the intention, the motives, social condition of the defendant). As a consequence; there is no average decision, nor a possible estimation. The defendant shall pay according to the decision of the judge.

Account compromise	Article 7 of Law 109/91	Accessing a system without authorisation and with intent to gain an illegitimate benefit or advantage for the agent or for a third party. Please note that the mere hacking (which lacks the referred intention) is not punishable.	Imprisonment of up to 1 year or a fine of up to 120 days Imprisonment of up to 3 years or a fine if the access is achieved by breaking security rules For these penalties, procedures are dependent upon a prior complaint Imprisonment from 1 year to 5 years in the following cases: - If the undue benefit is EUR 17,800 or more; - If the agent gains access to commercial or industrial secrets or confidential data protected by law The attempt is also punishable
Intrusion attempt	Article 7 of Law 109/91	Attempting to access a system without authorisation and with intent to gain an illegitimate benefit or advantage for the agent or for a third party. Please note that the mere hacking (which lacks the referred intention) is not punishable.	Imprisonment of up to 1 year or a fine ofup to 120 days Procedures are dependent upon a complaint
Unauthorised access to information	Article 7 of Law 109/91	Accessing a system without authorisation and with intent to gain an illegitimate benefit or advantage for the agent or for a third party.	Imprisonment of up to 1 year or a fine of up to 120 days Imprisonment of up to 3 years or a fine if the access is achieved by breaking security rules For these penalties, procedures are dependent upon a prior complaint Imprisonment of 1 year to 5 years in the following cases: - if the undue benefit is EUR 17,800 or more; - if the agent gains access to commercial or industrial secrets or confidential data protected by law

	Article 8 of Law 109/91	Intercepting a communication process within a system without authorisation using technical devices	Imprisonment of up to 3 years or a fine Attempt shall also be punishable
	Article 44 of Law 67/98 Code	Unlawfully obtaining access to personal data.	Imprisonment of up to 1 year or a fine of up to 120 days For this penalties, procedures are dependent upon a prior complaint The penalty shall be increased to double the maximum when access: (a) is achieved by means of violating technical security rules; (b) allows the agent or third parties to obtain knowledge of the personal data; (c) provides the agent or third parties with a benefit or material advantage
Unauthorised access to transmissions	Article 8 of Law 109/91	Intercepting a communication process within a system without authorisation using technical devices	Imprisonment of up to 3 years or a fine Attempt shall also be punishable
Unauthorised modification of information	Mainly Article 6 of Law 109/91	Modifying, erasing, or suppressing data or computer programmes or by other means intervening in a system, with intent to impede or disturb the functioning of a computer system or a distance communication data system	Imprisonment of up to 3 years or a fine of up to 600 days If the damage ranges between EUR 4,450 and EUR 17,799, the penalty is from 1 year of imprisonment up to 5 years of imprisonment If the damage is EUR 17,800 or more, the penalty is from 1 year of imprisonment up to 10 years of imprisonment
	Depending on object the intention of the agent: Article 5 of Law 109/91	Intentionally causing the non-usability of data, in order to gain an illegitimate benefit for the agent or third party	Imprisonment of up to 3 years or a fine. If the damage ranges between EUR 4,450 and EUR 17,799, the penalty is up to 5 years of imprisonment If the damage is EUR 17,800 or more, the penalty is from 1 year of imprisonment up to 10 years of imprisonment Attempt shall also be Punishable

Unauthorised access to communication systems	Article 6 of Law 109/91	Modifying, erasing, or suppressing data or computer programmes or by other means intervening in a system, with intent to impede or disturb the functioning of a computer system or a distance communication data system	Imprisonment of up to 3 years or a fine of up to 600 days If the damage ranges between EUR 4,450 and EUR 17,799, the penalty is from 1 year of imprisonment up to 5 years of imprisonment If the damage is EUR 17,800 or more, the penalty is from 1 year of imprisonment up to 10 years of imprisonment
Spam	Article 22 of Decree-Law n° 7/2004	Using electronic mail for advertising purposes without the prior, free, specific and informed consent of the addressee (it this is a physical person) Messaging to legal persons is allowed but recipients are entitled to opt-out. In case the company is included in the opt-out list, spamming is forbidden.	Spamming is considered an administrative offence, punished with a fine from EUR 2,500 to EUR 50,000. When the offence is committed by a legal person, the fine shall be increased by one-third in respect of both its maximum and minimum amount. Negligence is also punishable.

21.2 Law enforcement bodies

21.2.1 Police (www.pj.pt)

Portuguese police is divided into several police entities. The police has police stations all over Portugal. All stations are competent to receive a criminal complaint. However, the Judicial Police (*Polícia Judiciária*) is the entity mostly specialised in these areas of crime, in particular its Central Investigations Section for IT and Telecommunications Crime (*Secção Central de Investigação de Criminalidade Informática e Telecomunicações* - SCICIT). This section is based in Lisbon, and its agents cover the Portuguese territory, with the cooperation if necessary of unspecified police forces. It assists the prosecutor's department, providing technical and logistics support, and also aiding in obtaining evidence.

21.2.2 Courts

Criminal acts are decided mainly by first instance Criminal Courts (although the courts are not named Courts of First Instance). Against their decisions, appeal can be lodged with the Court of Appeal (*Tribunal da Relação*). The Supreme Court (*Supremo Tribunal de Justiça*) only hears points of law, which is also the case with the Constitutional Court (*Tribunal Constitucional*).

21.3 Reporting

21.3.1 Competent authorities

The *Secção de Investigação de Criminalidade Informática e Telecomunicações* (SCICIT) should be alerted in all cases of computer crime, where the victim is considering to file a complaint.

21.3.2 Contact details

For computer crimes complaints:

Gabinete Nacional da Interpol
Rua Gomes Freire, nº 213,
3º 1050-178 Lisboa
T: +351 21 359 58 00
F: +351 21 357 58 44
E: dcci.gni@pj.pt
Languages: Portuguese, English

Secção Central de Investigação de Criminalidade Informática e Telecomunicações
(SCICIT)
Rua Alexandre Herculano 42-A
1250-011
Lisboa
T: +351 18 64 39 00
F: +351 21 316 01 31
E: dciccef@pj.pt
W: www.pj.pt
Languages: Portuguese

For spamming complaints:

National Commission for Data
Protection (*Comissão Nacional de Protecção de Dados* - CNPD)
Rua de São Bento 148,
3º 1200 Lisboa
T: +351 21 392 84 00
F: +351 21 397 68 32
E: geral@cnpd.pt
W: www.cnpd.pt
Languages: Portuguese, English

21.3.3 Other reporting mechanisms

- There is no centralised structure to register specific types of unlawful acts, nor types of cyber attacks, nor has the regulator set up a similar system.

- Furthermore, Portugal did not enforce ISPs providing services in Portugal to adopt harmonized actions to combat computer crimes, or crimes outside the scope of the Law 109/91 (like the spread of illicit contents).

21.4 Forensics

Computer crime evidence in Portugal criminal procedure has no specific provision and all kinds of evidence may be submitted. Electronic evidence is admitted as a common form of evidence. The more authentic the evidence, the easier it will be to convince a judge during proceedings.

In the event of a computer crime procedure, SCICIT will carry out the initial inquiry and forensics under the supervision of the public prosecutor. Upon receipt of the report from the SCICIT or within the investigation procedure, the prosecutor may order additional inquiry measures. For certain investigation measures such as searches, the examining magistrate (*Juiz de Instrução*) has exclusive competence. In some cases, a prosecutor or judge will use a civil expert to assist the production of evidence.

Although not specifically set out, the following specific computer crime investigation measures are available:

21.4.1 House searching and seizure

This can include the removal of computer systems from the defendant's premises.

21.4.2 Data seizure

Upon the performance of house searching and seizure, decided by the judge, the prosecutor may decide to make a copy of the hard disk to put it on a hard disk at a forensic workstation. If necessary, (part of) the access to the data and the copies thereof may be blocked or the data may even be deleted, e.g. because it is impossible to make a copy or in case of viruses. Seized data is admissible as documentary evidence and supporting evidence. In the case of documentary evidence, they are backed up by other material evidence and declarations of the suspects and witnesses.

21.4.3 Network searching

The investigating magistrate may order a search of the network if deemed necessary.

21.4.4 Involvement of experts

The investigating magistrate may order persons who have the necessary expertise to provide information on the working of the relevant informatics system or on how to get access to the relevant electronic data. These experts may be referred to as formal experts in the criminal hearing. The Portuguese State is liable for damage to the computer system or to the data as a result of these investigating measures, if not decided by the judge.

21.5 References

- Criminal Code (1982, mostly amended in 1995) and Code of Criminal Procedure [1987, but this code has undergone several amendments)
- Law 109/91 of 17 August 1991 concerning computer crimes (*Lei da Criminalidade Informática)*
- Law 24/96 of 31 July 1996, concerning the protection of consumers (*Lei do Consumidor*)
- Law 67/98 of 26 October 1998, concerning data protection (*Lei de Protecção de Dados Pessoais*)
- Decree-Law n.º 7/2004 of 7 January 2004, concerning spamming (*Lei do Comércio Electrónico*)
- Law no. 41/2004 of 18 August 2004, concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Lei n.º 41/2004, de 18 de Agosto*)

CHAPTER 22 Country report – Slovak Republic

22.1 Slovak legislation on computer crimes

The Slovak Criminal Code is still developing, reacting to and reflecting the development of new forms of computer crime. Its evolution occurred in several reforms, of which the broadest was the one in 1991, which included computer and network related offences by introducing Section 257a (Damaging or Misusing Data Carrier Records). This is why most of the incidents described below fall under one of the provisions of this section. In some cases other sections of the Criminal Code can be relevant such as Section 152 (Infringement of Copyright), Section 178 (Unauthorised Processing of Personal Data), Section 182 (Damaging and Endangering of Operation of Public Interest Advices), Section 239 (Infringing on the Confidentiality of Transmitted Messages), Section 249 (Unauthorised Use of Other People's Items). The Criminal Code recognises only criminal acts committed by natural entities, not by legal entities.

There is no specific law dealing with the spreading of unsolicited commercial communication (spam), but this activity is partially treated by the Law on advertising (*Zákon o reklame,* No.147/2001). This law treats spam as an administrative tort rather than as a crime. The content of the spam may also be covered by the definition of unfair competition in the Commercial Code.

At the time of writing a brand new Criminal Code and Code of Criminal Procedure passed the third reading of the legislative process, but it has not yet entered into force because it hasn't been signed by the President. These two codes which reform criminal law in Slovakia should become effective on 1 January 2006.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	None as such	Only punishable as a preparatory act (attempt to commit another form of cyber crime)	Dependent on the subsequent behaviour: punishable as an attempt to commit another crime (e.g. theft, violation of house freedom acts of terrorism)
Malicious code	Section 257a Criminal Code	The intentional unauthorised accessing of data storage and altering or deleting the data, or making a change in the computer system in order to cause harm or gain profit for oneself or someone else	Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)

	Section 249 Criminal Code	Unauthorised use of other people's items	Imprisonment up to 1 year, a fine up to SKK 5,000,000 (approx. EUR 130,000), or prohibition of a specific activity. The penalty is raised to imprisonment between 6 months and three years when causing damage exceeding 20 times the minimum wage, i.e. SKK 130,000 (approx. EUR 3,300), prohibition of a specific activity, and a fine up to SKK 5,000,000 (approx. EUR 130,000). The penalty is raised to imprisonment between 1 year and five years if causing damage exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600), a fine up to SKK 5,000,000 (approx. EUR 130,000), or prohibition of a specific activity The penalty is raised to imprisonment between 2 year and 8 years if causing damage exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000)
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunications facility	Imprisonment up to 6 years or a fine up to SKK 5,000,000 (approx. EUR 130,000)

Denial of service	Section 257a Criminal Code	The intentional unauthorised accessing of data storage and altering or deleting the data, or making a change in the computer system in order to cause harm or gain profit for oneself or someone else	Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunications facility	Imprisonment up to 6 years or a fine up to SKK 5,000,000 (approx. EUR 130,000)
Account compromise	Section 257a Criminal Code	The intentional unauthorised accessing of data storage and altering or deleting the data, or making a change in the computer system in order to cause harm or gain profit for oneself or someone else	Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)

	Section 249 Criminal Code	Unauthorised use of other people's items	Imprisonment up to 1 year, a fine up to SKK 5,000,000 (approx. EUR 130,000), or prohibition of a specific activity. The penalty is raised to imprisonment between 6 months and three years when causing damage exceeding 20 times the minimum wage, i.e. SKK 130,000 (approx. EUR 3,300), prohibition of a specific activity, and a fine up to SKK 5,000,000 (approx. EUR 130,000). The penalty is raised to imprisonment between 1 year and five years if causing damage exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600), a fine up to SKK 5,000,000 (approx. EUR 130,000), or prohibition of a specific activity The penalty is raised to imprisonment between 2 year and 8 years if causing damage exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000)
Intrusion attempt	Section 257a juncto Section 8 Criminal Code	Attempt to gain access to a data carrier and unauthorized use of such data	Punishable as an accomplished crime. Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)

	Section 249 juncto Section 8 Criminal Code	Attempt to make unauthorised use of other people's items	Punishable as an accomplished crime. Imprisonment up to 1 year, a fine up to SKK 5,000,000 (approx. EUR 130,000), or prohibition of a specific activity. The penalty is raised to imprisonment between 6 months and three years when causing damage exceeding 20 times the minimum wage, i.e. SKK 130,000 (approx. EUR 3,300), prohibition of a specific activity, and a fine up to SKK 5,000,000 (approx. EUR 130,000). The penalty is raised to imprisonment between 1 year and five years if causing damage exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600), a fine up to SKK 5,000,000 (approx. EUR 130,000), or prohibition of a specific activity The penalty is raised to imprisonment between 2 year and 8 years if causing damage exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000)
Unauthorised access to information	Section 257a juncto Section 8 Criminal Code	Attempt to obtain unauthorised access to a data carrier and unauthorized use with the intention to cause harm, destroying, damaging or rendering useless of such data	Punishable as an accomplished crime. Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)

	Article 239 juncto Section 8 Criminal Code	Attempt of infringement of confidential transmitted messages of private communication or data communication with harmful intent.	Imprisonment of up to two years or a fine up to SKK 5,000,000 (approx. EUR 130,000). When committed by the provider or another competent person or when intentionally enabling some other person to commit this act, or when one of the aforementioned changes the content of the transmitted message the penalty is raised to imprisonment between 6 months and three years, and a fine up to SKK 5,000,000 (approx. EUR 130,000)
Unauthorised access to transmissions	Section 257a Criminal Code	Gaining access to a data carrier and making unauthorised use of such data with harmful intent	Punishable as an accomplished crime. Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)
	Section 239 Criminal Code	Infringing on the confidentiality of messages transmitted by telephone, telegraph or similar public facility	Imprisonment of up to two years or a fine up to SKK 5,000,000 (approx. EUR 130,000). When committed by the provider or another competent person or when intentionally enabling some other person to commit this act, or when one of the aforementioned changes the content of the transmitted message the penalty is raised to imprisonment between 6 months and three years, and a fine up to SKK 5,000,000 (approx. EUR 130,000)

	Section 240 Criminal Code	Disclosure of the contents of a confidential message or abuse of such message	Imprisonment up to 1 year, or prohibition of a specific activity, a fine up to SKK 5,000,000 (approx. EUR 130,000). When committed by the provider or another competent person or when intentionally enabling some other person to commit this act – imprisonment up to two years or prohibition of a special activity
	Section 240(a) Criminal Code	Unlawful production or receiving of technical means capable of enabling access to transmissions of communication by telephone, telegraph or other public communication facility	Imprisonment up to three years, a fine up to SKK 5,000,000 (approx. EUR 130,000) or forfeiture of a specific item. When the crime is committed in an organised group or when causing a serious damage exceeding 6 times the minimum wage, i.e. SKK 39,000 (approx. EUR 1,000), the penalty is raised to imprisonment between one and five years
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunications facility	Imprisonment up to 6 years or a fine up to SKK 5,000,000 (approx. EUR 130,000)
Unauthorised modification of information	Section 257a Criminal Code	Gaining access to a data carrier and making unauthorised use of such data with harmful intent	Punishable as an accomplished crime. Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)

Unauthorised access to communication systems	Section 257a Criminal Code	Gaining access to a data carrier and unauthorized use, destroying, damaging or rendering useless of such data, or interference with the hardware or software of a particular computer	Imprisonment between six months and three years, prohibition of a specific activity, forfeiture of a specific object. The penalty is raised to between one and five years when the crime is committed in an organised group or when causing serious damage or profit (exceeding 100 times the minimum wage, i.e. SKK 650,000 (approx. EUR 16,600). The penalty is raised to imprisonment between two and eight years when causing damage or profit exceeding 500 times the minimum wage, i.e. SKK 3,250,000 (approx. EUR 84,000) A fine up to SKK 5,000,000 (approx. EUR 130,000)
	Section 182(1)(a) Criminal Code	Impairing and endangering the operation of a public telecommunications facility	Imprisonment up to 6 years or a fine up to SKK 5,000,000 (approx. EUR 130,000)
Spam	Section3(6) Law on advertising	Using electronic mail to send automatically commercial communication without the prior consent of the recipient	(Administrative) fine up to SKK 2,000,000 (approx. EUR 52,000)
	Section 178(1) Criminal Code	Unauthorized processing of personal data	Imprisonment up to 1 year, a fine up to SKK 5,000,000 (approx. EUR 130,000), prohibition of a specific activity

22.2 Law enforcement bodies

22.2.1 Police (www.minv.sk)

The police of the Slovak republic consists of the National police presidium (*Prezídium policajného zboru*) and 8 regional police district directorates (*Krajské riaditeľstvá policajného zboru*). There are two special departments dealing with computer crime.

At the National police presidium, the Criminal police and investigation service (*Úrad justičnej a kriminálnej polície*) was created, including a Division of economical crime

(*Odbor ekonomickej kriminality*), along with a special Department for fighting forgery and computer crime (*Oddelenie boja proti falšovaniu a počítačovej kriminalite*), which is responsible for monitoring and investigating criminal activities related to information technology. Its tasks include securing evidence on the Internet, service activities and providing support to the Divisions of economical crime which are created on the level of each regional police district. The latter are responsible for monitoring and investigating criminal activities related to information technology on a regional and district level. They can also cooperate with organisations such as The Business Software Alliance.

22.2.2 Office of the Public Prosecution (*Generálna prokuratúra Slovenskej republiky*) (www.genpro.gov.sk)

The office of the public prosecution is an independent hierarchically structured singular system of state authority lead by the General attorney (*Generálny prokurátor*) that is responsible for the protection of rights and legally protected interests of natural persons, legal entities and the state. The organisational structure of the office of the public prosecution corresponds with the structure of the courts, but not with the division of state regional administrations at the regional level.

On the lowest level, it is divided into 45 regional offices (*okresné prokuratúry*) of the public prosecution and 3 department military offices (*obvodné vojenské prokuratúry*), while the second level consists of 8 county offices (*krajské prokuratúry*) and a higher military office (*vyššia vojenská prokuratúra*). A subsection of the office is made up of the Special office of the public prosecution (*Špeciálna prokuratúra*) which deals with particular crimes such as corruption, particularly significant crimes and also crimes committed by organised groups or terrorists.

22.2.3 Courts (www.justice.gov.sk)

The court most likely to deal with computer crime is the District Court, criminal section (*Okresný súd, trestný senát, samosudca*).

Against the decisions of the District Court, appeal can be lodged with the Regional Court (*Krajský súd*), while the Upper Higher Court (*Najvyšší súd*) will rule on any appeal against a decision of the Regional Court acting as a court of first instance.

The Regional Court (*Krajský súd*), criminal section (*trestný senát*) is competent as a court of first instance in more serious cases where the relevant crime can be punished with a minimum imprisonment of eight years.

The Special Court (*Špeciálny súd*) deals with the same crimes as the special office of public prosecution.

The Supreme Court (*Najvyšší soud*) decides in extraordinary legal remedies against appellate court decisions. It also evaluates final enforceable decisions of the courts and on their basis and in the interest of the uniformity of courts' decision-making adopts standpoints on the courts decision-making in particular matters.

22.2.4 Office for Personal Data Protection (www.statnydozor@pdp.gov.sk)

The Office for Personal Data Protection (*Úrad na ochranu osobných údajov*) as a state organ takes part in the protection of elementary rights and liberties of natural persons concerning the processing of their personal data. It executes its tasks and duties independently and in accordance with the law.

It has limited rights to investigate infractions against the law on Personal Data Protection (*Zákon o ochrane osobných údajov*), and it has the right to issue an administrative fine of up to 10,000,000 SKK (approx. 256,000 EUR).

Any fines imposed for these offences are decided upon by the Office following the regulations in the Code of Administrative Procedure.

22.3 Reporting

22.3.1 Competent authorities

The police should be alerted in all cases of computer crime, such as denial of service attacks, hacking, fraud and any major computer crime incidents including software piracy and illegal content offences.

During its supervision of personal data protection the Office for Personal Data Protection also makes use of notifications and grievances from legal entities and natural persons concerning suspected infractions against this law. Reports to the office are lodged in writing.

Everyone who has received a spam message can address a report to one of four organs of government supervision:

- the Slovak Agricultural and Food Administration (*Slovenská poľnohospodárska a potravinárska inšpekcia*) is in charge of supervision of advertisement for food and similar commodities

- the State Institute for Control of Pharmaceuticals (*Štátny ústav pre kontrolu liečiv*) supervises advertisements of pharmaceuticals and nursing products and similar additional products
- the State institute for Control of Veterinary Pharmaceuticals (*Štátny ústav pre kontrolu veterinárnych liečiv*) supervises advertisements of veterinary pharmaceuticals
- in all other cases the responsible organ is the Slovak Trade Commission (*Slovenská obchodná inšpekcia*).

22.3.2 **Contact details**

Ministry of Interior of the Slovak Republic
(MINISTERSTVO VNÚTRA SR)
Pribinova 2, 812 72 Bratislava
T: +421 2 509 41 111
F: +421 2 509 44 397
M: tokmv@minv.sk

National police presidium (*Prezídium policajného zboru*)
POLICAJNÁ LINKA DÔVERY:
T: +421 2 555 71 110
F: +421 9 610 44 028
M: tokmv@minv.sk
Languages: Slovak, English

Generálna prokuratúra Slovenskej republiky
Štúrova 2
812 85 Bratislava
T: +421 2 595 31 111
M:generalna.prokuratura@genpro.gov.sk
Languages: Slovak, English

Office for Personal Data Protection
(*Úrad na ochranu osobných údajov Slovenskej republiky*)
Odborárske námestie č. 3
817 60 Bratislava 15

Kancelária predsedu úradu :
T: +421 2 502 39 418
F: +421 2 502 39 441
M: statny.dozor@pdp.gov.sk
Languages: Slovak, English

Supreme Audit Office SR
(*Najvyšší kontrolný úrad SR*)
Priemyselná 2
824 73 Bratislava 26
T: +421 2 554 23 69 / +421 2 554 24 628
F: +421 2 555 66 835
M: info@sao.gov.sk

22.3.3 **Other reporting mechanisms**

The Slovak Republic, unlike many other European countries, has no special system, unit or mechanisms for collecting reports on computer crimes. The Office for Personal Data Protection collects reports on infractions regarding the protection of personal data. The Slovak Trade Commission handles reports of unsolicited advertisements through standard channels, email and telephone desk, paper forms or through interchange of information between state bodies. Information on other computer crimes is collected by the Police of the Slovak Republic, including information about child pornography, racism or terrorist behaviour.

Consequently, content related crimes should be reported to one of the local police units.

Illicit content – Child pornography and incitement to racial hatred are examples of explicitly forbidden Internet content in the Slovak Republic.

Harmful content – With regard to content that can generally be harmful to Internet users, in particular children, no specific legislation exists so far.

However, several related alert mechanisms exist in the Slovak Republic:

- The Business Software Alliance offers a telephone hotline (0800 152 152) and an online alert mechanism (www.bsa@bsa.sk) for the reporting of illegal software.
- International Federation of the Phonographic Industry – represents and protects the rights of producers of acoustic and musical audio-visual recordings and represents the interests of its members. Copyright infractions can be reported to +421 2 529 23 886, or via e-mail (ifpi@ifpi.sk).

22.4 Forensics

Evidence in criminal proceedings is regulated by the Code of Criminal Procedure (*Trestý poriadok)*. All kinds of evidence may be submitted except for evidence gathered by threat or use of unlawful coercion. The more authentic the evidence, the easier it will be to convince a judge during proceedings. Electronic documents have become a common evidence type in recent judicial practice.

The role of the police organs in general is to examine criminal complaints and investigate criminal acts. The police organs act independently and on their own initiative, however they may require the prosecutor's (*prokurátor*) permission for certain measures, especially when these interfere with civil rights.

With respect to computer crimes, the investigating organ may use a civil expert to assist in the investigation.

There are no specific computer crime investigation measures defined in the Code of Criminal Procedure. However, a number of provisions may be applied by analogy.

The following investigation measures are available:

22.4.1 Obligation to yield an object

Anyone who is in possession of an object relevant for the purposes of the criminal proceedings is under the obligation to yield that object to the court upon request by either a prosecutor or a police organ. If it has to be retained for the purposes of the criminal proceedings, the person is obliged to render it upon request.

22.4.2 Seizure of an object

When an object important for criminal proceedings is not yielded upon request by the person who possesses it, it can be seized at the request of either a prosecutor or police organ. The police organ requires the prior agreement of the prosecutor before such a warrant can be issued.

22.4.3 Domiciliary and personal search, search of other areas and estates, admittance to the dwelling, other areas and estates

Domiciliary searches can be conducted when there are reasonable grounds to believe that the home or other living area contains an object important for criminal proceedings, or that a suspect is hiding there.

22.4.4 Interception and recording of telecommunications traffic

During criminal proceedings an order for the interception and recording of telecommunications traffic may be issued when there are reasonable grounds to believe that the facts to be revealed are significant for criminal proceedings.

An order for the interception and recording of telecommunications traffic is issued in writing before the beginning of the criminal proceedings and in pre-trial by the judge at the request of the prosecutor.

The period of interception and recording may not occupy more than six months. The period may be prolonged by the judge for another period of six months.

22.4.5 Expert involvement

When expert knowledge is necessary to clarify an element important for the criminal proceedings, the investigating organ in criminal investigations and the judge in legal proceedings may decide to involve an expert.

In certain special cases demanding particular academic arbitration, the investigating authority may decide to request a state organ or institute to provide an expertise or to examine a previously delivered expertise.

22.5 References (www.just.fgov.be)

- Criminal Code (*Trestýí zákon*, Law No. 140/1961 Coll.)
- Code of Criminal Procedure (*Trestý poriadok*, Law No. 141/1961 Coll.)
- Act on Certified Experts, Translators and Interpreters (*Zákon o znalcoch, tumočníkoch a prekladateľoch*, Law No. 382/2004 Coll.)
- Code of Administrative Procedure (*Správny poriadok*, Law No. 71/1967 Coll.)
- Personal Data Protection Act (*Zákon o ochrane osobných údajov*, Law No. 428/2002 Coll.)
- Electronic Communication Act (*Zákon o elektronických komunikáciách*, Law No. 610/2003 Coll.)
- Electronic Trade Act (*Zákon o elektronickom obchode*, Law No. 22/2004 Coll.)
- Advertisement Act *(Zákon o reklame,* Law No. 147/2002)

CHAPTER 23 Country report - Slovenia

23.1 Slovenian legislation on computer crimes

Changes to the Criminal Code in 2004 amended three articles that directly deal with computer crime (unauthorised entry into an information system, information system break-in, and the manufacture and acquisition of arms and instruments used for committing criminal acts). These cover a wide range of computer-related criminal acts. Data retention and lawful interception are covered in the Electronic Communications Act (*Zakon o elektronskih komunikacijah)*, which also penalises spam (unsolicited communication). A similar provision against spam can also be found in the Consumer Protection Act (*Zakon o varstvu potrošnikov)*. Additionally, the Electronic Commerce and Electronic Signatures Act (*Zakon o elektronskem poslovanju in elektronskem podpisu*) penalises security breaches related specifically to certification authorities for digital certificates.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	None as such	Could only be used to show preparatory activities and possible intent after criminal offence has been performed.	None.
Malicious code	Article 309, §3 Criminal Code	Possession, manufacturing, selling, making available for use, importing, exporting or in any other way providing devices for breaking into or unlawfully entering an information system with intent to commit a criminal offence.	Imprisonment of up to 1 year.

Denial of service	Article 225, § 2 Criminal Code	Obstructing transfer of data or operation of an information system without authorisation.	Imprisonment of up to 2 years. If the offence resulted in a large loss of property, the penalty is raised to imprisonment from 3 months up to 5 years.
	Article 242, § 1 Criminal Code	Obstructing transfer of data or operation of an information system [in the course of business operations and without authorisation] in order to obtain unlawful pecuniary benefit, or to cause pecuniary damage to another.	Imprisonment of up to 3 years. If the offence resulted in a large loss of property or a large property benefit (or if such was the perpetrators intent), the penalty is raised to imprisonment of up to 5 years.
Account compromise	Article 225, § 1 Criminal Code	Accessing an information system without authorisation.	A fine between EUR 125 and EUR 12,500, or a fine of EUR 37,500 if the crime is committed for one's own interest.[28]
Intrusion attempt	Article 225, §3 Criminal Code	Attempt to perform a criminal offence as defined in Article 225, §2	Imprisonment of up to 2 years. If the offence resulted in a large loss of property, the penalty is raised to imprisonment from 3 months up to 5 years.
Unauthorised access to information	Article 154, § 2 Criminal Code	Breaking into a computer database in order to acquire personal data	A fine[28] or imprisonment of up to 1 year.
	Article 225, §2 Criminal Code	Use without authorisation of data held in an information system.	Imprisonment of up to 2 years. If the offence resulted in a large loss of property, the penalty is raised to imprisonment from 3 months up to 5 years.
	Article 242, §1 Criminal Code	Use of data held in an information system [in the course of business operations and without authorisation] in order to obtain an unlawful pecuniary benefit, or to cause pecuniary damage to another.	Imprisonment of up to 3 years. If the offence resulted in a large loss of property or a large property benefit (or such was the perpetrators' intent), the penalty is raised to imprisonment up to 5 years.
Unauthorised access to transmissions	Article 225, §1 Criminal Code	Intercepting data of a non-public nature that is being transferred to or from an information system.	A fine between EUR 125 and EUR 12,500, or a fine of EUR 37,500 if the crime is committed for one's own interest (see footnote 28 on page 237).

[28] Fines are defined by Article 38 of Penal Code and define fixed limits for one-off amounts as well as for daily installments which take into account the perpetrator's daily income calculated from the last three months net income. Amounts mentioned here are for one-off payments.

	Article 150, §2 Criminal Code	Intentionally learning of the content of a message transmitted by telephone or any other means of telecommunications, by use of technical means	A fine or imprisonment of up to 1 year (see footnote 28 on page 237).
Unauthorised modification of information	Article 225, §2 Criminal Code	Modifying data stored within an information system or obstructing the transfer of data without authorisation.	Imprisonment of up to 2 years. If the offence resulted in a large loss of property, imprisonment from 3 months up to 5 years.
	Article 242, §1 Criminal Code	Changing data held in an information system or obstructing the transfer of data [in the course of business operations and without authorisation] in order to obtain unlawful pecuniary benefit, or to cause pecuniary damage to another.	Imprisonment of up to 3 years. If the offence resulted in a large loss of property or a large property benefit (or such was the perpetrators' intent), the penalty is raised to imprisonment of up to 5 years.
Unauthorised access to communication systems	Article 225, §1 Criminal Code	Accessing an information system without authorisation.	A fine between EUR 125 and EUR 12,500, or a fine of EUR 37,500 if a crime is committed for one's own interest (see footnote 28 on page 237).
Spam	Article 109, §1 Electronic Communicatio ns Act	Use of electronic mail for the purpose of direct marketing is only allowed if the subscribers have given their prior consent.[29]	A fine between EUR 8,333 and EUR 41,667 for legal entities (defined in Article 152).
	Article 45.a, §1 Consumer Protection Act	A company may use electronic commercial mail only with the prior consent of the consumer who the message is intended for.[30]	A fine of up to EUR 12,500 for legal entities. A fine of up to EUR 4,167 for natural persons (as defined in Article 77).

[29] §2 of the same article allows direct marketing to one's customers, provided they include clear opt-out mechanism: "… natural persons or legal entities that obtain electronic mail addresses from the customers of their products or services may use such addresses for direct marketing of their similar products or services, but they shall be obliged to give their customers the possibility at any time, free of charge and using simple means, of preventing such use of their electronic address."

[30] Since by definition a "consumer" can only be an individual person acting on his/her own behalf, this act concerns only spam directed to personal e-mail addresses (and not to addresses of persons acting on behalf of legal entity where they are employed). The Electronic Communications Act, Article 109 thus provides a broader regulation for spam.

23.2 Law enforcement bodies

23.2.1 Police (www.policija.si)

The Slovenian police consists of a General Directorate (state level, *Generalna policijska uprava*), 11 Police Directorates (regional level, *Policijska uprava*) and Police Stations (local level, *Policijska postaja*). Police Stations perform community policing. Investigation of criminal activity is performed by a regional Police Directorate and in general reports of observed criminal activity should be directed at the appropriate regional Police Directorate. The General Directorate on a state level includes within its Criminal Investigation Police (*Uprava kriminalistične policije*) the Computer Crime and Criminal Analysis Unit (*Sektor za računalniško kriminaliteto in kriminalistično analitiko*), which can assist in any particular investigation.

23.2.2 Courts (www.sodisce.si)

44 Local Courts (first instance courts, *okrajno sodišče*) handle less serious criminal cases and civil cases concerning claims for damages or property rights up to a certain value. 11 District Courts (also first instance courts, *okrožno sodišče*) handle criminal and civil cases which exceed the jurisdiction of local courts, juvenile criminal cases and copyright and intellectual property cases. Against decisions of local and district courts, appeal can be lodged with a Higher Court (*višje sodišče*). The Supreme Court (*vrhovno sodišče*) is the highest court in the state.

23.3 Reporting

23.3.1 Competent authorities

Criminal activities covered by the Criminal Code should be reported to the appropriate regional Police Directorate or local Police Station. For reports originating in other countries, reports should be directed to the appropriate law-enforcement body in that country and will then be forwarded to the appropriate law-enforcement body in Slovenia through official channels.

Reports on Electronic Communications Act violations are handled by the Agency for Post and Electronic Communications (*Agencija za pošto in elektronske komunikacije*), while violations of the Consumer Protection Act are handled by the Market

Inspectorate of the Ministry of Economy (*Tržni inšpektorat RS pri Ministrstvu za gospodarstvo*).

23.3.2 **Contact details**

Agency for Post and Electronic Communications
(Agencija za pošto in elektronske komunikacije RS)
Stegne 7, p.p. 418
1001 Ljubljana
Slovenia
Tel : +386 1 583 63 00
Fax : +386 1 511 11 01
E-mail : info.box@apek.si
Web : http://www.apek.si/

Market Inspectorate
(Tržni inšpektorat RS)
Parmova 33
1000 Ljubljana
Slovenia
Tel: +386 1 280 8700
Fax: +386 1 280 8740
E-mail: tirs.info@gov.si
Web: http://www2.gov.si/mg/tirs/tirs.nsf

23.3.3 **Other reporting mechanisms**

The Slovenian Computer Emergency Response Team (SI-CERT) handles and coordinates reports on security incidents involving computer networks in Slovenia. SI-CERT can also provide assistance and advice on reporting criminal activity to the appropriate Slovenian law-enforcement body. Another role that SI-CERT performs is the issuing of warnings to the general public on security issues via public bulletins and advisories.

SI-CERT (ARNES)
Jamova 39, p.p. 7
1001 Ljubljana
Slovenia
Tel : +386 1 479 88 22
Fax : +386 1 479 88 23
E-mail : si-cert@arnes.si
Web : http://www.arnes.si/si-cert/

Most Slovenian ISP's are members of SISPA (Slovenian Internet Service Providers Association), which is organised within the Slovenian Chamber of Commerce. SISPA also runs a working group on network and information security.

No specific mechanism for reporting illicit or harmful content yet exists, although a project for a specialised hotline is being drafted at the time of this writing. Until such a body is established, reports on such content should be submitted to the police, either directly or via SI-CERT.

23.4 Forensics

Handling of electronic evidence material in Slovenian criminal procedure is not specifically regulated. Such materials are admitted as a common form of evidence. Investigation measures can include seizure of data and equipment, analysis of traffic data and lawful interception of communication for specific criminal offences. In all cases the appropriate court order must be presented, either to the owner of the material to be seized, or to the ISP that records traffic data or can implement lawful interception of communication.

Common practice of data seizure is that two exact copies are made. One is sealed and stored for possible future reference, while the other is used for forensic analysis. The original hardware is then often returned to the owner. Whether data is returned in full or is partially wiped depends on the nature of the offence and the nature of data itself.

23.5 References

- Criminal Code (*Kazenski zakonik RS, 2004*)
- Electronic Communications Act *(Zakon o elektronskih komunikacijah, 2004)*
- Electronic Commerce and Electronic Signature Act *(Zakon o elektronskem poslovanju in elektronskem podpisu, 2004)*
- Consumer Protection Act *(Zakon o varstvu potrošnikov, 2004)*
- Criminal Procedure Act *(Zakon o kazenskem postopku, 2004)*

CHAPTER 24 Country report - Spain

24.1 Spanish legislation on computer crimes

The Spanish Criminal Code entered in force on 24 May 1996. Although it has been subject to several amendments, it already took into consideration specific computer crimes such as damages inflicted to data, computer related frauds or the protection of reserved personal data stored in files, computer systems and electronic or means.

Organic Law 15/2003 of 25 November 2003 has significantly amended the Criminal Code, modifying some computer related crimes and introducing others. Amongst them, it newly regulates the misuse of devices, punishes the mere possession of child pornography and the so-called virtual child pornography, modifies the crimes related to intellectual property, or slightly raises the pecuniary limits between crime and misdemeanour in relation to computer fraud and damages.

As far as Target Fingerprinting, account compromise or intrusion attempt are concerned, it is important to note that the Spanish Criminal Code does not punish the mere access to computer systems or equipment with no other specific intention. Such acts may only be punishable in case of intent to commit another cyber-crime.

Finally, the Law on Information Society Services and Electronic Commerce (*Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico)* established a provision imposing data retention obligations on operators and service providers of electronic communications. However, the provision needs further development by a Royal Decree so as to be enforceable. In addition, the Law on Information Society Services and Electronic Commerce as well as the Organic Law on Personal Data Protection (*Ley Orgánica de Protección de Datos de Carácter Personal)* penalises the sending of unsolicited commercial communications via e-mail or using equivalent means of communications (e.g. SMS).

Relevant Incidents	Applicable provision[31]	Description	Sanction
Target Fingerprinting	None as such	Only punishable as an intent to commit another form of cyber-crime	Dependent on the subsequent behaviour: punishable as an intent to commit another crime
Malicious code	Article 264 Criminal Code	Destroying, altering, making useless or in any way damaging data, programs or documents in computer networks, systems or media.	Imprisonment between 1 and 3 years and a fine (12 to 24 months)[32] of up to EUR 288,000.
	Article 560 Criminal Code	Causing damages that interrupt, hinder or destroy telecommunication lines or facilities	Imprisonment between 1 and 5 years
	Article 413 Criminal Code	Totally or partially taking away, destroying, making useless or hiding documents (committed by the public authority or civil servant keeping them in connection with the duties of his or her office)	Imprisonment between 1 and 4 years, a fine (7 to 24 months) of up to EUR 288,000 and deprivation of the right to exercise public office between 3 to 6 years
	Article 584 Criminal Code	Making useless information classified as secret or reserved, capable of causing detriment to national security or defence (committed by a Spanish citizen with the intent to help a foreign country or an international organisation or association)	Imprisonment between 6 and 12 years
Denial of service	Article 264.2 Criminal Code	Destroying, altering, making useless or in any way damaging another's person data, programs or documents in computer networks, systems or media.	Imprisonment between 1 and 3 years and a fine (12 to 24 months) of up to EUR 288,000.
	Article 560 Criminal Code	Causing damages that interrupt, hinder or destroy telecommunication lines or facilities	Imprisonment between 1 and 5 years

[31] Due to the scope of the present work, reference will be made mainly to crimes regulated in the Criminal Code, but not to misdemeanours or other crimes regulated in the Military Criminal Code.

[32] The Criminal Code determines for each offence the period for which the fine shall be paid. The judge or court shall then specify the amount to be paid per day over the established period, which may vary between EUR 2 to 400. For calculation purposes, it is presumed that a month has 30 days and a year 360 days.

	Article 413 Criminal Code	Totally or partially taking away, destroying, making useless or hiding documents (committed by the public authority or civil servant keeping them in connection with the duties of his or her office)	Imprisonment between 1 and 4 years, a fine (7 to 24 months) of up to EUR 288,000 and deprivation of the right to exercise public office between 3 to 6 years
	Article 584 Criminal Code	Making useless information classified as secret or reserved, capable of causing detriment to national security or defence (committed by a Spanish citizen with the intent to help a foreign country or an international organization or association)	Imprisonment between 6 and 12 years
	Article 598 Criminal Code	Making useless information classified as secret or reserved capable of causing detriment to national security or defence	Imprisonment between 1 and 4 years
Account compromise	None as such	Only punishable as an intent to commit another form of cyber-crime	Dependent on the subsequent behaviour: punishable as an intent to commit another crime
Intrusion attempt	None as such	Only punishable as an intent to commit another form of cyber-crime	Dependent on the subsequent behaviour: punishable as an intent to commit another crime
Unauthorised access to information	Article 197 Criminal Code	Seizure of another's person papers, letters, e-mail, messages or any other documents[33] or personal effects with the intent to discover secrets or to breach the privacy of the victim	Imprisonment between 1 and 4 years and a fine (12 to 24 months) of up to EUR 288,000
			Imprisonment between 2 years and 6 months to 4 years, and a fine (18 to 24 months) of up to EUR 288,000 when the act affects sensitive data,[34] the victim is a minor or legally incapacitated, or there is intent to profit.
			Imprisonment between 4 and 7 years when both sensitive data is affected and there is intent to profit.
		Unauthorised access by any means, seizure or use of reserved personal or	Imprisonment between 1 and 4 years and a fine (12 and 24 months) of up to EUR 288,000

[33] According to Article 26 of the Criminal Code, a document is any physical medium containing data or facts relevant for evidential or legal purposes.

[34] That is, ideology, religion, beliefs, health, race, or sexual life

		family data stored in files, computer systems, electronic means or in any other public or private archive or record, causing detriment to the data subject or to a third party	Imprisonment between 2 years and 6 months to 4 years and a fine (18 to 24 months) of up to 288,000 EUR when the act affects sensitive data, the victim is a minor or legally incapacitated, or there is intent to profit.
			Imprisonment between 4 and 7 years if both sensitive data is affected and there is intent to profit.
		Unauthorised access to information [art. 197 Criminal Code], committed by those responsible or in charge of the files, computer and electronic means, archives or records	Imprisonment between 3 and 5 years
			Imprisonment between 4 and 5 years when the act affects sensitive data, the victim is a minor or legally incapacitated, or there is intent to profit.
			Imprisonment between 4 and 7 years if both sensitive data is affected and there is intent to profit.
	Article 198 Criminal Code	Unauthorised access to information [art. 197 Criminal Code], committed by public officers or civil servants	Imprisonment between 2 years and 6 months to 4 years and a fine (18 to 24 months) of up to EUR 288,000 The penalty is increased to imprisonment between 4 and 5 years when committed by those responsible or in charge of the files, computer and electronic means, archives or records
			Imprisonment between 3 years and 3 months to 4 years and a fine (21 to 24 months) of up to EUR 288,000, when the act affects sensitive data, the victim is a minor or legally incapacitated, or there is intent to profit The penalty is increased to imprisonment between 4 years and 6 months to 5 years when committed by those responsible or in charge of the files, computer and electronic means, archives or records
			Imprisonment between 5 years and 6 months to 7 years if both sensitive data is affected and there is intent to profit The penalty is increased to imprisonment between 6 years and 3 months to 7 years committed by those responsible or in charge of the files, computer and electronic means, archives or records

			Deprivation of the right to exercise public functions between 6 and 12 years
	Article 200 Criminal Code	Committing the crime described in article 197 Criminal Code resulting in the discovering, revealing or disclosing of reserved data of legal persons without the consent of their legal representatives	Imprisonment between 1 and 4 years and a fine (12 to 24 months) of up to EUR 288,000 The penalty is increased to imprisonment between 2 years and 6 months to 4 years and a fine between 18 to 24 months when there is intent to profit
			Imprisonment between 3 and 5 years when committed by those responsible or in charge of the files, computer and electronic means, archives or records The penalty is increased to imprisonment between 4 and 5 years when there is intent to profit
	Article 278 Criminal Code	Seizure of data, documents, electronic means or related objects with the intent to unveil secrets of companies	Imprisonment between 2 and 4 years and a fine (12 to 24 months) of up to EUR 288,000
	Article 415 Criminal Code	Unauthorised intentional access to secret documents by the public authority or civil servant keeping them in connection with the duties of his or her office	A fine (6 to 12 months) of up to EUR 144,000 and deprivation of the right to exercise public functions between 1 and 3 years
	Article 416 Criminal Code	Unauthorised intentional access to secret documents kept by private persons on behalf of the Government or public authority or civil servant	A fine (3 to 6 months) of up to EUR 72,000
	Article 584 and 586 Criminal Code	Access to information classified as secret or reserved, capable of causing detriment to national security or defence with the intent to help a foreign country or an international organization or association	Imprisonment between 6 and 12 years when committed by a Spanish citizen and between 3 and 6 years when committed by a foreigner domiciled in Spain.
	Article 598 Criminal Code	Access to information classified as secret or reserved capable of causing detriment to national security or defence	Imprisonment between 1 and 4 years
Unauthorised access to transmissions	Article 197.1 Criminal Code	Interception of telecommunications and the use of technical means	Imprisonment between 1 and 4 years and a fine (12 and 24 months) of up to EUR 288,000

		to listen, transmit, or record any communication signal with the intent to discover secrets or to breach the privacy of the victim	Imprisonment between 2 years and 6 months to 4 years and a fine (18 to 24 months) of up to EUR 288,000 when the act affects sensitive data, the victim is a minor or legally incapacitated, or there is intent to profit.
			Imprisonment between 4 and 7 years if both sensitive data is affected and there is intent to profit.
	Article 198 Criminal Code	Unauthorised access to transmissions [art. 197 Criminal Code], committed by public officers or civil servants	Imprisonment between 2 years and 6 months to 4 years and a fine (18 to 24 months) of up to EUR 288,000 The penalty is increased to imprisonment between 4 and 5 years when committed by those responsible or in charge of the files, computer and electronic means, archives or records
			Imprisonment between 3 years and 3 months to 4 years and a fine (21 to 24 months) of up to EUR 288,000, when the act affects sensitive data, the victim is a minor or legally incapacitated, or there is intent to profit The penalty is increased to imprisonment between 4 years and 6 months to 5 years when committed by those responsible or in charge of the files, computer and electronic means, archives or records
			Imprisonment between 5 years and 6 months to 7 years if both sensitive data is affected and there is intent to profit The penalty is increased to imprisonment between 6 years and 3 months to 7 years committed by those responsible or in charge of the files, computer and electronic means, archives or records
			Deprivation of the right to exercise public functions between 6 to 12 years
	Article 278 Criminal Code	Interception of telecommunications and the use of technical means to listen, transmit, or record any communication signal with the intent to unveil secrets of companies	Imprisonment between 2 and 4 years and a fine (12 to 24 months) of up to EUR 288,000

	Article 536 Criminal Code	Interception of telecommunications and the use of technical means to listen, transmit, or record any communication signal by a public authority, civil servant or agent infringing legal or constitutional rights	Deprival of the right to exercise public functions between 2 to 6 years
Unauthorised modification of information	Article 264 Criminal Code	Destroying, altering, making useless or in any way damaging another's person data, programs or documents in computer networks, systems or media.	Imprisonment between 1 and 3 years and a fine (12 to 24 months) of up to EUR 288,000
	Article 197 Criminal Code	Unauthorised altering or modification of reserved personal or family data stored in files, computer systems, electronic means or in any other public or private archive or record, causing detriment to the victim or to a third party	Imprisonment between 1 and 4 years and a fine (12 to 24 months) of up to EUR 288,000
	Article 390 and 391 Criminal Code	Altering essential elements of an existing document or including false statements committed by public authority or civil servant acting in the course of his or her duties	Imprisonment between 3 and 6 years, a fine (6 to 24 months) of up to EUR 288,000 and deprivation of the right to exercise public functions between 2 and 6 years
			A fine (6 to 12 months) of up to EUR 144,000 and deprivation of the right to exercise public functions between 6 month and 1 year in case of gross negligence
	Article 392 Criminal Code	Altering essential elements of an existing document or including false statements	Imprisonment between 6 months and 3 years and a fine (6 to 12 months) of up to EUR 144,000
	Article 395 Criminal Code	Altering essential elements of an existing document or including false statements with the intent to cause harm	Imprisonment between 6 months and 2 years.
	Article 413 Criminal Code	Totally or partially taking away, destroying, making useless or hiding documents by the public authority or civil servant keeping them in connection with the duties of his or her office	Imprisonment between 1 and 4 years, a fine (7 to 24 months) of up to EUR 288,000 and deprivation of the right to exercise a public office between 3 to 6 years
Unauthorised access to communication systems	Article 255 Criminal Code	Committing telecommunications fraud using mechanisms installed for that purpose or using any other clandestine medium and causing damage higher than 400€	A fine (3 to 12 months) of up to EUR 144,000

	Article 256 Criminal Code	Unauthorised use of telecommunications terminal equipment causing damage higher than 400€	A fine (3 to 12 months) of up to EUR 144,000
	Article 286 Criminal Code	Use of equipment or programs that allow the unauthorised access to telecommunication equipments	A fine (3 to 12 months) of up to EUR and publication of the judgement in Official Gazettes.
Spam	Article 21 of the Law on Information Society Services and Electronic Commerce	The use of electronic mail or similar systems for advertising or promotional purposes, without the consent of the recipient	Fine of up to EUR 150,000

24.2 Law enforcement bodies

24.2.1 Police (www.policia.es)

The BIT (*Brigada de Investigación Tecnológica*), created in 2001, is the police division in charge of technological investigations and new forms of committing criminal offences, such as: threats, insults or false accusations by electronic mail, SMS, discussion forums and web pages; child pornography; fraud using communication systems; access and removals of data, discovery and disclosure of secrets; or piracy, amongst others.

24.2.2 Guardia Civil (www.guardiacivil.org)

The Group of Computer Crimes (*Grupo de delitos telemáticos*) was created in 1997, and has been a member of INTERPOL since October 1997. It deals with the investigation of crimes such as: confidentiality of and access to data and computer systems; child pornography; Internet and telecommunications fraud; or crimes related to intellectual and industrial property, amongst others.

24.2.3 Courts (www.poderjudicial.es)

Competence of the different judges or courts depends on several criteria such as territoriality, functionality, capacity of the offender, etc. The court most likely to carry out the pre-trial investigation is the examining magistrate (*Juez de Instrucción*). If the case goes to trial, the court most likely to deal with computer crime is the Penal Court (*Juzgado de lo Penal*). Against its decisions, appeal can be lodged with the Provincial Court (*Audiencia Provincia*l). The Supreme Court (*Tribunal Supremo*) only hears points of law.

24.3 Reporting

Centro Policial de Canillas
C/ Julián González Segador s/n
28043 - Madrid

General enquiries:
T. +34 91 582 27 47
delitos.tecnológicos@policia.org;

Frauds related to telecommunications:
T. +34 91 582 27 48
delitos.telecomunicaciones@policia.es;

Child Pornography:
T. +34 91 582 27 53
denuncias.pornografia.infantil@policia.es;

Frauds:
T. +34 91 582 27 54
fraudeinternet@policia.es;

Virus, attacks, logical security:
T. +34 91 582 27 52
seguridad.logica@policia.es;

Piracy:
T. +34 91 582 27 51
antipirateria@policia.es

GROUP OF COMPUTER CRIMES
Dirección General de la Guardia Civil
C/ Guzman el Bueno 110
28003 - Madrid
Tel. +34 90 010 00 62 / General enquiries: Tel. +34 90 010 10 62
sugerencias@guardiacivil.org

24.3.1 **Other reporting mechanisms**

- www.alerta-antivirus.red.es

  It is a service offered by Red.es, the public entity empowered to assign domain names under the `.es´ ccTLD, to manage the Spanish domain names register, and to foster the development of the telecommunications and the Information Society in Spain. Red.es manages a platform (*Centro de Alerta Temprana sobre Virus Informáticos*), which makes available to users and security experts information on viruses and their characteristics. They give useful hints on viruses and security problems (consultas@alerta-antivirus.es) and improvement of services (sugerencias@alerta-antivirus.es).

- www.protegeles.com

  Protegeles is a non-profit association fighting against child pornography on the Internet. It is a hotline for reporting child pornography offences that closely collaborates with law enforcement bodies in important police operations at national and international level. It also carries out campaigns to improve the security and privacy of minors on the Internet.

- www.agpd.es

The Spanish Data Protection Agency is a public body with its own legal personality and unlimited public and private legal capacity, which acts fully independently in the performance of its tasks. It is the national supervisory authority with regard to data protection.

24.4 Forensics

The Spanish criminal procedure is mainly oral; the judge shall have direct access to evidence so as to assess it correctly. However, electronic evidence is admitted as a common form of evidence. It may be introduced in the procedure directly or through witnesses, such as the public authorities or law enforcement agencies that directly accessed the evidence.

The initial inquiry and forensics are carried out by the police under the supervision of the public prosecutor, who shall guarantee the rights of the offender as well as those of the victim. The public prosecutor may order additional inquiry measures and make the decision on whether or not to pass the investigation on to an examining magistrate (*Juez de Instrucción*).

The following specific computer crime investigation measures are available:

24.4.1 Data seizure

The entry and search of public buildings and premises requires an order issued by a judge, while the entry and search of domiciles requires the consent of the concerned person or – in its absence – a reasoned Judicial Decree. However, police agents may exceptionally enter, search, and seize items, in which case such circumstance shall be communicated to the judge indicating the reasons thereof and the results obtained. As a rule, the search and seizure shall take place in presence of the clerk of the judge and of the concerned party, his or her legal representative, a relative, or two neighbours. It is possible and convenient to have a technical person assisting the search of computers or seizure of electronic data. Additionally, the search and seizure shall avoid unnecessary interferences, which may be achieved by the use of filtering tools for accessing data.

As a preventive measure, the judge may – from the moment at which the entry, register, or seizure is authorised – adopt any adequate measure to avoid the removal or destruction of documents or instruments.

24.4.2 Network searching

The judge may order the surveillance of communications used for criminal purposes. As a rule, the interception shall not last longer than three months, but the mentioned term maybe renewed. Likewise, the Ministry of the Interior may order the interception of communications when the investigation is related to terrorism, but such circumstance shall be communicated immediately to a judge, who shall confirm or revoke the measure within 72 hours.

24.5 References

- Criminal Code approved by Organic Law 10/1995 of 23 November (*Código Penal*).
- Criminal Procedure Law approved by Royal Decree of 14 September 1882 (*Ley de Enjuiciamiento Criminal*).
- Organic Law 6/1985 on the Judiciary (*Ley Orgánica del Poder Judicial).*
- Law 34/2002 of 11 July on Information Society Services and Electronic Commerce (*Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico).*
- Organic Law 15/1999 of 13 December on Personal Data Protection (*Ley Orgánica de Protección de Datos de Carácter Personal).*

CHAPTER 25 Country report - Sweden

25.1 Swedish legislation on computer crimes

Offences against the Confidentiality, Integrity and Availability of information in Sweden are mainly managed through the Swedish Criminal Code and in particular through chapter 4 which deals with "Crime Against Liberty and Peace", chapter 12 which deals with "Crime Inflicting Damage", and chapter 13 that deals with "Crimes Involving public Danger".

Chapter 4 of the Swedish Criminal Code is the one most frequently used to handle these CIA offences. Sec 8 deals with the *"breach of postal or telecommunications secrecy*": it is a provision dealing with unauthorised access to a communication or its unauthorised interception.

Other provisions relating to these offences are sec 9, 9a and 9c of the same chapter. In particular, sec 9 deals with *"intrusion into a safe depository*" establishing that it is an offence to open letters or telegrams or to otherwise obtain access to something kept under seal or lock or otherwise enclosed.

Sec 9a establishes that it is an offence to unlawfully and secretly listen to or record by technical means for sound reproduction, speech in a room, a conversation between others or discussions at a conference or other meeting to which the public is not admitted and in which the person doing the listening has improperly obtained access. All these conducts are defined as *"eavesdropping"*.

Sec 9 c deals with the *"breach of data secrecy"*, the case in which a person unlawfully obtains access to record automatic data processing activities or unlawfully alters or erases or inserts such a recording device.

Chapter 12 of the Swedish Criminal Code deals with the infliction of damage: the first section deals with persons who destroy or damage property to the detriment of another's right thereto. The penalty provided is a fine or a term of imprisonment up to one year. The third section of the article deals with serious cases of inflicting damage. Damage is to be considered serious when it causes a risk to anyone's life or health, or when the damage was to something of great cultural or financial importance. In this case the penalty is a term of imprisonment of up to 4 years.

Another important chapter of the Swedish Criminal Code that has to be taken into consideration in relation to these sorts of offences is Chapter 13 which deals in general with "Crimes Involving Public Danger."

Chapter 13 Sec 4 establishes that a person who destroys or damages property of considerable importance for the defence of the Realm, public subsistence, the administration of justice or public administration, or for the maintenance of public order and security in the Realm, or who by some other action, not limited to the withholding of labour or encouraging such action, seriously disrupts or obstructs the use of such property, shall be sentenced for sabotage.

This provision also applies to anyone who destroys or damages or seriously disrupts or obstructs public traffic or the use of telegraph, telephone, radio or other similar public services, or the use of an installation for the supply of water, light, heat or power to the public. The penalty for this offence is a term of imprisonment up to 4 years.

Sec 5 of Chapter 13 deals with the serious sabotage, a sabotage that could cause serious danger to the Realm, or to the lives of a number of persons or to property of special importance. The penalty for this offence is a term of imprisonment from 2 to 10 years or life.

Currently Sweden is undertaking great efforts to harmonise its legislation towards the Council of Europe Convention on Cyber crime and the EU legal framework decision.

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine[35] or imprisonment for at most two years.
	Criminal Code, chapter 4, sec 10	Attempted breach of data secrecy	Fine or imprisonment for at most two years.
Malicious code	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine or imprisonment for at most two years.
Denial of service	Criminal Code, chapter 8, sec 8	Unlawful dispossession	Fine or imprisonment for at most six months
Account compromise	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine or imprisonment for at most two years.
Intrusion attempt	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine or imprisonment for at most two years.
	Criminal Code, chapter 4, sec 10	Attempted breach of data secrecy	Fine or imprisonment for at most two years.
Unauthorised access to information	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine or imprisonment for at most two years.
	Criminal Code, chapter 4, sec 10	Attempted breach of data secrecy	Fine or imprisonment for at most two years.
Unauthorised access to transmissions	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine or imprisonment for at most two years.
Unauthorised modification of information	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine or imprisonment for at most two years.
Unauthorised access to communication systems	Criminal Code, chapter 4, sec 9c	Breach of data secrecy	Fine or imprisonment for at most two years.
Spam	Marketing Practices Act, sec 13 b	Administrative provision	No sanction, but if an infringement continues after an order of termination of behaviour, a fine may be issued.

25.2 Law enforcement bodies

25.2.1 Police (www.polisen.se)

[35] Fine amounts are not fixed in Swedish law. The fine is based on, among any other relevant factor, the judge's estimation and the yearly income of the perpetrator.

A great emphasis is placed on the computer crime awareness of individual law enforcement officers in Sweden. All officers are given a basic understanding of computer crime and dealing with computer evidence (at a basic level) when they pass through Police College.

At the local level, there are 21 independent state police departments which cover distinguished geographic regions. In each unit there are 1 or 2 specially trained investigators. This number can be higher in the major departments with other local experts being present. Furthermore, each regional state unit is able to call upon the national unit for support if required. The IT crime squad forms part of the National Criminal Investigation Department (*Rikskriminalpolisen*). There are 15 officers in the Squad, who are a mix of police officers and special profile technicians. The IT Crime Squad (*IT-brottsroteln*) is divided into subunits concerned with search and seizure and interne surveillance, which mirrors the structure of other national units (e.g. the UK NHTCU).

The responsibilities and supportive measures are first and foremost directed to local police units in each state department, but also to international liaisons, specifically with Interpol, Europol and the G-8 24/7 reporting points. This unit does not, however, cover national intelligence related liaisons regarding computer crime, which is handled by the Swedish Security Service (*Säkerhetspolisen*, Sweden's internal intelligence agency).

In the Swedish National Forensic Laboratory (*Statens kriminaltekniska laboratorium*) there are five engineering staff who deal exclusively with computer forensics. They are a resource that can be called upon by the National unit and state forces.

The Police College programme includes a basic level of digital and computer evidence awareness in basic training, but a special 13 week course also exists for specialist investigators. This consists of a 10 week introductory course with regards to computing and information technology, covering operation of Information Technology at an advanced level. A further 3 weeks provide training on legal considerations, software and forensic tools. Other advanced training courses are available on a topical basis (e.g. the rise in popularity of Distributed Denial of Service attacks). Opportunities are available for CSSIP qualification, but as the state departments pay for this, it is not mandatory.

The level of sophistication is quite high, and outside civilian experts are only called in 5 to 6 times a year for specific assistance on investigations. The IT Crime Squad also co-operates with the military, intelligence services and other national research agencies. This co-operation is normally along the lines of seminars and workshops as well as the more obvious operational assistance.

25.2.2 Courts (www.domstolsverket.se)

Sweden has two parallel types of court - general courts, which deal with criminal and civil matters, and general administrative courts, which deal with administrative matters. There are three levels of general courts - the district courts (*tingsrätt*), the courts of appeal (*hovrätt*) and the Supreme Court (*Högsta domstolen*). There are also three levels of administrative courts – the county courts (*länsrätt*), the administrative courts of appeal (*kammarrätt*) and the Supreme Administrative Court (*Regeringsrätten*).

25.3 Reporting

25.3.1 Competent authorities

The IT Crime Squad is the national and international contact point regarding cases of computer crime. Within the squad there is an IT incident coordination unit (*Samordningsfunktion - brottsrelaterade IT-incidenter*) which is a formal cooperation between the National Criminal Police and the Security Service. Upon contacting the IT Crime Squad on any case concerning computer crime, the unit will take action and route the case to the proper investigative resources.

Issues concerning the Personal Data Act are dealt with by the Swedish Data Inspection Board (*Datainspektionen*).

25.3.2 Contact details

IT Crime Squad
National Criminal Police
Box 12256
SE-102 26 Stockholm,
Sweden
T: +46 (0)8 401 45 90
F: +46 (0)8 650 77 78
E: itbrott@rkp.police.se
W: http://www.polisen.se
Languages: Swedish, English, Finnish

Datainspektionen (Data Inspection Board)
Box 8114
SE-104 20 Stockholm
Sweden
T: +46 (0)8 657 61 00
F: +46 (0)8 652 86 52
E: datainspektionen@datainspektionen.se
W: www.datainspektionen.se

25.3.3 Other reporting mechanisms

The most important reporting initiative for securing information systems and networks is the Swedish IT Incident Centre (SITIC – http://www.sitic.se). SITIC's task is to support society in improving protection against IT incidents. SITIC facilitates exchange of information regarding IT incidents between organisations in society, and disseminates information about new problems which can potentially impede the functionality of IT systems. In addition, SITIC provides information and advice regarding proactive measures and compiles and publishes statistics.

There are also a few alert mechanisms for content related crimes. The most important mechanism targets child pornography, and is managed by the National Criminal Police and the unit specifically dealing with child pornography. The unit can be contacted through e-mail (childabuse@rkp.police.se).

25.4 Forensics

A free or informal system of evidence exists in Sweden. This proves to be both a benefit and a problem for law enforcement as anything digital in nature can be submitted, and the burden of proof rests on the evidence itself rather than adherence to procedural stipulations. Hence decisions can go one way or the other and are more acutely dependent on the testimony and performance of expert witnesses in explaining the relevance of the written evidence to the judge and jury.

Digital evidence in Sweden can be submitted under standard documentary evidence rules or as separate evidence (in the case of computer code or programs, for example). In the testimony of both law enforcement and expert witnesses, the need to preserve confidentiality about methods (particularly regarding encryption) is specifically highlighted in police training.

Internally within the Police, digital evidence and computer forensic best practice is taken from the Interpol Computer Crime Manual and a Swedish version, published by the National Police College called 'The Handbook for Search and Seizure'. Furthermore, use is made of an Interpol handbook on Internet monitoring.

25.5 References

- Swedish Criminal Code (*Brottsbalken*)
- (http://www.regeringen.se/content/1/c4/15/36/d74ceabc.pdf)

- Swedish Code of Judicial Procedure (*Rättegångsbalken*)
- (http://www.regeringen.se/content/1/c4/15/40/472970fc.pdf)
- Swedish Electronic Communications Act (*Lagen om elektronisk kommunikation*)
- (http://www.pts.se/Archive/Documents/EN/The_Electronic_Communications_Act_2003_389.pdf)
- Act on Responsibility for Electronic Bulletin Boards (*Lag om ansvar för elektroniska anslagstavlor*)
- (http://www.sweden.gov.se/content/1/c6/02/61/42/43e3b9eb.pdf)
- Personal Data Act (*Personuppgiftslagen*) (http://www.datainspektionen.se/pdf/ovrigt/pul-eng.pdf)
- Market Law in Sweden (extract) (*Marknadsföringslagen*)
- (http://www.english.konsumentverket.se/mallar/en/artikel.asp?lngCategoryId=665)

CHAPTER 26 Country Report - United Kingdom

26.1 UK legislation on computer crimes

England and Wales are common law countries. The most distinctive feature of a common law country is that judge made law remains an important source of law[36]. This is in contrast to civil law countries that have codified their laws with the result that legislation is the only source of law. There are many areas of English and Welsh law which have been codified or where case law has been overridden by express legislation. Scotland is not a common law jurisdiction, but generally uses the same criminal legislation as England and Wales and is increasingly tending towards a mix of common law and those on the statute books.

English law also generally applies to Northern Ireland.

Much of what is conventionally labelled "computer crime" can be prosecuted in the English courts by the use of regular statutes and case law. Thus: a "computer fraud" is prosecuted under the law of deception within the various Theft Acts; child pornography is prosecuted under the Protection of Children Act 1978, as amended. Much law reform is achieved by modifying and extending exist law to cope with new situations rather than by the introduction of completely new legislation. This can sometimes make it difficult to find a single place where the whole of an area of law is clearly set out. Criminal lawyers use a reference book called "Archbold" to assist them.

[36] Common law is developed by individual judicial decisions. This is known as case law and precedent. Where a legal issue has been decided by a superior court lower courts are bound to follow it in subsequent cases. Free/Informal evidentiary rules exist in the UK. There is no Criminal Code (since there is no written Constitution) but case law determines criminal activity, in addition to substantive law contained within thematic legislation.

The Computer Misuse Act (CMA) was enacted in 1990. It remains the primary piece of UK legislation focusing on the misuse of computer systems. It covers crimes such as hacking and the deliberate spread of viruses, and was created to prevent unauthorised access to or modification of computer systems and to deter criminal elements from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer.

In 2004, MPs – specifically, the All-Party Internet Group (APIG) – began a review of the CMA, on the basis that this legislation was created before the emergence of the Internet and therefore required updating. The Act was seen to focus too much on standalone computers and not enough on computer networks. In addition some of the definitions used in the 1990 Act need updating. The final report outlined several recommendations to the government for changes to the CMA.[37]

In March 2005, APIG called for amendments to the CMA to address the threat from DOS attacks.

An updated version of the CMA will be better valued if it combines various security regulations relevant for standalone and network situations.

[37] See http://www.apig.org.uk/CMAReportFinalVersion1.pdf for the report

Relevant Incidents	Applicable provision	Description	Sanction
Target Fingerprinting	Ripa 2000[38]: Section 1	Intentional and unauthorized interception of any communication in the course of its transmission by means of public postal service or a public telecommunication system.	A fine and/or up to 2 years imprisonment
	CMA Section 2[39]	Cause a computer to perform any function with the intention of securing access to any program or data held in a computer, if this access is unauthorised and if this is known at the time of causing the computer to perform the function.	A fine and/or up to 6 months imprisonment
Malicious code	CMA Section 3[40]	Have the knowledge and intentionally cause the unauthorized modification of the contents of any computer.	A fine and/or a term of imprisonment of up to 5 years
Denial of service	CMA Section 3	Have the knowledge and intentionally cause the unauthorized modification of the contents of any computer.	A fine and/or a term of imprisonment of up to 5 years. Not all forms of Denial of Service may be covered by s 3 CMA
Account compromise	CMA Section 1[41] or Theft Acts	Cause a computer to perform any function with the intention of securing access to any	A fine and/or a term of imprisonment not exceeding 6 months

[38] Regulation of Investigatory Powers Act 2000

[39] CMA Section 2 supposes that the intention to commit such an offence need not be directed at a particular program or data; at a program or data of any particular kind; or at a program or data held in any particular computer.

[40] CMA Section 3 supposes that the intention is understood to include the modification of the contents of any computer and by so doing impair the operation of any computer, prevent or hinder access to any program or data held in any computer or impair the operation of any such program or the reliability of any such data.

The intention to commit such an offence need not be directed at a particular program or data; at a program or data of any particular kind; or at a program or data held in any particular computer.

The knowledge includes knowledge that any modification caused is unauthorized, regardless of whether this is, or is intended to be, permanent or temporary.

		program or data held in a computer, if this access is unauthorised and if this is known at the time of causing the computer to perform the function. Prosecutors may however prefer to charge as fraud rather than as a "computer" offence	
Intrusion attempt	CMA Section 1	Cause a computer to perform any function with the intention of securing access to any program or data held in a computer, if this access is unauthorised and if this is known at the time of causing the computer to perform the function.	A fine and/or a term of imprisonment not exceeding 6 months
Unauthorised access to information	None as such	The UK does not have specific "Trade Secrets" or "Industrial Espionage" legislation; prosecution is via *modus operandi*	
Unauthorised access to transmissions	RIPA 2000 Section 1	Intentional and unauthorized interception of any communication in the course of its transmission by means of public postal service or a public telecommunication system.	A fine and/or a term of imprisonment of up to 2 years
Unauthorised modification of information	CMA Section 3	Have the knowledge and intentionally cause the unauthorized modification of the contents of any computer.	A fine and/or a term of imprisonment up to to 5 years

[41] CMA Section 1 supposes that the intention to commit such an offence need not be directed at a particular program or data; at a program or data of any particular kind; or at a program or data held in any particular computer.

Unauthorised access to communication systems	CMA Section 1	Cause a computer to perform any function with the intention of securing access to any program or data held in a computer, if this access is unauthorised and if this is known at the time of causing the computer to perform the function.	A fine and/or a term of imprisonment not exceeding 6 months
Spam	2003 Regulations from EC Directive on Privacy and Electronic Communications.[42]	Unsolicited marketing material cannot be transmitted by e-mail to an individual subscriber (a consumer) unless the recipient has previously notified the sender, that s/he consents, for the time being, to receive such communications. Exceptions a) The recipient has actively invited the communication via a third party. b) The recipient has been made aware s/he is likely to receive marketing messages but has not, for the time being, objected to receiving them (through a simple and clear method). Marketing e-mails (whether solicited or unsolicited) cannot be transmitted to any subscriber (whether corporate or individual) where a) the identity of the sender has been disguised or concealed, or b) a valid address to which the recipient	Possible fine of £5000 for each breach, or an unlimited fine if the trial is before a jury.

[42] Statutory Instrument 2003 No. 2426 Crown Copyright 2003 - http://www.hmso.gov.uk/si/si2003/20032426.htm Accessed 31 March 2005

		can send an opt-out request has not been provided.	

26.2 Law Enforcement Bodies

26.2.1 Police

Traditionally policing in the UK has been based on local control with a few national entities. There are 43 forces in England and Wales, including the largest force: the Metropolitan Police. There are 8 forces in Scotland.Other major forces include the British Transport Police who are responsible for the policing of the UK Rail Network. The Force is also responsible for policing the London Underground and some smaller local metro and tram systems.The Police Service of Northern Ireland (formerly the Royal Ulster Constabulary or RUC) covers Northern Ireland.

Smaller and more localised computer incidents are examined in the first instance by these bodies.The main national body is the National High Tech Crime Unit (NHTCU) which is part of the National Crime Squad and is staffed by officers from a number of law enforcement agencies, including the military.NHTCU is in the course of becoming part of a new entity, the Serious and Organised Crime Agency, SOCA.

26.2.2 Courts

In England and Wales simpler cases are heard in lower courts known as Magistrates' Courts. These are presided over either by lay justices who are assisted by professional Clerks or by full-time District Judges. Magistrates' Courts do not have juries.

More serious and complex cases are heard in the Crown Courts. These are presided over by judges who act as chairmen of events and articulate the law. The prosecution and the defence cases are presented by lawyers (barristers). Juries decide on the basis of facts and instructions on the law given by the judge.

Appeals are heard in the first instance by the Court of Appeal with a final appeal to the House of Lords.

Computer crime cases are heard in exactly the same way as regular criminal trials.

26.3 Reporting

26.3.1 Competent Authorities

The National Hi-Tech Crime Unit (NHTCU), which is part of the National Crime Squad, provides a national capability to deal with computer crime. NHTCU was formed in April 2001 to be the central point of contact for cyber-crime investigations. The Unit

also undertakes a liaison role with other computer crime units in UK regional police forces (Constabularies).

The Unit has four separate arms:

1. · Investigations
2. · Intelligence
3. · Tactical and Technical Support
4. · Digital Evidence (Forensic Retrieval)

The NHCTU can also call upon the resources of national intelligence agencies and research organisations if required – specifically QinetiQ (formerly part of the Defence Evaluation and Research Agency) and DSTL (Defence Science and Technology Laboratories) and the Government Communications Head Quarters (GCHQ).

The NHTCU has established a Confidential Reporting Charter designed to allay concerns voiced by businesses and commercial organisations that notification of computer security incidents will invariably result in adverse publicity. This has had some success of late, and the Unit is putting much effort into outreach to commercial stakeholders.

In addition to the national unit, there are individual Computer Crime Units, dealing with Computer and Content related crimes, in each constabulary. The most experienced of these is the Metropolitan Police's Computer Crime Unit.

The Metropolitan Police Unit is part of the Specialist Crime operational command unit within the Metropolitan Police's Specialist Operations Command. The Computer Crime Unit works together with other specialist units, both within the Metropolitan Police and at a national and international level.

26.3.2 **Contact Details**

National Hi-Tech Crime Unit
PO Box 10101
London E14 9NF
T: +44 (0)870 241 0549
F: +44 (0)870 241 5729
E: admin@nhtcu.org
W: www.nhtcu.org

Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
T: 01625 545 740
01625 545 745
F: 01625 524 510
E: data@dataprotection.gov.uk
W: http://www.informationcommissioner.gov.uk

26.3.3 **Other reporting mechanisms**

In addition to the formal channels through Law Enforcement there are a number of additional reporting processes being established. Chief of these is the Warning Advice and Reporting Point (WARP) concept, developed by the National Infrastructure Security Co-

ordination Centre (NISCC). London Connects (an organisation designed to deliver e-Government to Greater London) has piloted the first WARP. NISCC itself provides a reporting channel for the collection of intelligence, particularly from critical industry sectors.

The Internet Watch Foundation (IWF) is an independent body responsible for reporting of illegal (child pornography or criminally racist) content but it has no direct policing role.

The Information Commissioner can be referred to in the instance of the use and exploitation of personally identifiable information. Similarly, local Trading Standards bodies afford some level of consumer protection in regard to online activities (goods and services).

26.4 Forensics

Evidence collection is governed by the Police and Criminal Evidence Act 1984 (PACE 84) and other legislation. Guidelines are set out in publications such as the ACPO 'Good Practice Guide for Computer Based Evidence' and the Interpol Computer Crime Manual.

Computer evidence is widely accepted in the criminal justice system and has been used in many prosecutions.Generally speaking in the UK, computer evidence falls under the same rules as other evidence,

> '...the onus is on the prosecution to show to the court that the evidence produced is no more and no less than when it was first taken into the possession of police.'

The ACPO Good Practice Guide states that investigators should be careful to ensure that no data change takes place on media that is expected to be relied upon in court. No access of original data must take place and all investigative work must be completed on an image of the drive. In circumstances where it is necessary to access original data held on a target computer, the person doing so must be competent to do so and must be prepared to give evidence explaining his actions. The guide establishes that care must be taken to preserve a chain of custody and an audit trail of all process applied to computer based evidence, which should be examinable by a third party who should be able to come to the same result. Responsibility for adherence to these principles is placed with the principle investigating officer.

NHTCU has two separate areas of note in relation to forensics:

- Network monitoring: Monitoring and investigation of traffic in a dynamic real time environment.

Hard disk investigation: Forensic procedures based around the forensic examination of seized hard disks.

There is a high degree of expertise in forensic investigation in the United Kingdom and several universities run special courses for forensic investigators. In addition, law

enforcement can call upon a dynamic and thriving commercial market of forensic investigation specialists as well as formidable national resources held by national intelligence agencies.. Much forensic work is carried out by police units and a handful of private sector companies. The UK Forensic Science Service maintains some expertise in digital evidence. , A scheme to accredit digital forensic examiners by the Council for the Registration of Forensic Practitioners started in late 2005.

26.5 References

- Computer Misuse Act 1990;
- Regulation of Investigatory Powers Act 2000

"Revision of the Computer Misuse Act" Report of an Inquiry by the All Party Internet Group, June 2004 – http://www.apig.org.uk/CMAReportFinalVersion1.pdf Accessed 31 March 2005

- "Latest Guidance on Anti-Spam Legislation", Business Gateway - http://www.bgateway.com/topical_information.asp?pageId=2.4.2.12 Accessed 31 March 2005
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 -

http://www.hmso.gov.uk/ Accessed 31 March 2005

- "The Computer Misuse Act 1990" Home Office - http://www.homeoffice.gov.uk/crime/internetcrime/compmisuse.html Accessed 31 March 2005
- "Reform of the Computer Misuse Act 1990" Internet Crime Forum, 30th April 2003 - http://www.internetcrimeforum.org.uk/cma-icf.pdf Accessed 31 March 2005
- "e-Business Factsheet: E-Mail Marketing, Spam and the Law", Services to Businesses by Scottish Enterprise - http://www.scottish-enterprise.com/publications/europeanprivacylaw.pdf Accessed 31 March 2005