

# **MISUSE OF THE INFORMATION HIGHWAY**

*Criminal sanctions and some legal remedies*

**Aron Mifsud Bonnici**

Thesis submitted in partial fulfilment of the degree of Doctor of Laws

**Faculty of Laws  
University of Malta**

**June 1997**

## **Abstract**

As society becomes increasingly dependant on information technology it becomes essential to analyse and update traditional legal concepts and established offences. Large networks such as the Internet provide new venues for and new forms of criminal activity. An awareness of what makes up the Internet is, therefore, essential.

Traditional offences, particularly those having an economic character, are today being committed in cyberspace with greater ease and impunity. Thus, amendments to present laws becomes essential so as to confirm their application in the computer world.

On the other hand, the phenomenon of large-scale computer communications has created forms of abuse which were previously unknown. Of particular relevance is the activity of hackers, which may range from mere nuisance to outright sabotage. It is imperative that programs and data are given a degree of protection similar to other 'traditional' property. Some States have enacted special legislation to criminalise such activity but others are still to address the threat.

A major issue, presently the subject of international debate, is that of Internet content. Many have expressed concern about the exposure of minors to questionable material which is available online. Others are particularly sensitive to proposals of Internet censorship. There have already been some largely-unsuccessful attempts in this respect and it may well be that the solution does not lie in banning content but in filtering it. Maltese law does regulate pornography but, possibly, it may fail to address the main concern.

The new means of processing and storing of information could mean that the detection of crime is more difficult. One should examine to what extent law enforcement officials may be prevented from investigating offences committed on or through the use of information technology equipment. In particular, new cryptographic technology may render the authorities' efforts futile and one should see whether it is desirable to control the availability and use of encryption.

Cyberspace acknowledges no national boundaries and is largely unconcerned with state sovereignty. The application of law in cyberspace therefore offers a great challenge to traditional rules of territoriality. International co-operation and consensus is probably the only way to a practical solution.

## **Table of Contents**

<b>Abstract</b> .....	<b>2</b>
<b>Table of Contents</b> .....	<b>3</b>
<b>Table of Authorities</b> .....	<b>5</b>
<b>Tables and figures</b> .....	<b>6</b>
<b>Acknowledgements</b> .....	<b>7</b>
<b>Abbreviations</b> .....	<b>8</b>
<b>INTRODUCTION</b> .....	<b>9</b>
<b>1. AN OVERVIEW</b> .....	<b>13</b>
1.0 Introduction.....	13
1.1 The information infrastructure.....	13
1.1.1 The Internet .....	14
1.1.2 Other networks .....	22
1.2 Main legal instruments .....	23
<b>2. COMPUTER-RELATED FRAUD AND FORGERY</b> .....	<b>28</b>
2.0 Introduction.....	28
2.1 Computer fraud .....	29
2.1.1 Definition .....	30
2.1.2 Comparative analysis .....	38
2.1.3 Pyramid and other fraudulent schemes .....	40
2.2 Computer forgery .....	42
2.2.1 Comparative analysis .....	47
<b>3. HACKING</b> .....	<b>52</b>
3.0 Introduction.....	52
3.1 The Council of Europe Recommendation.....	59
3.2 The United Kingdom and Singapore Acts.....	63
3.2.1 Unauthorised access.....	63
3.3 Legislative approaches to criminalisation .....	68
3.3.1 'System-entry' approach .....	68
3.3.2 'Data-espionage' approach.....	69
3.3.3 'Breach of security' approach.....	70
3.4 'Initially authorised' access .....	71
3.5 Possession of hacking tools.....	74
<b>4. UNAUTHORISED MODIFICATION</b> .....	<b>77</b>
4.0 Introduction.....	77
4.1 Damage to data and programs .....	77
4.1.1 The Council of Europe Recommendation .....	78
4.1.2 Comparative analysis .....	80
4.2 Viruses .....	89

<b>5. ILLEGAL AND HARMFUL CONTENT.....</b>	<b>95</b>
5.0 Introduction.....	95
5.1 Illegal and harmful content.....	97
5.1.1 Illegal content.....	98
5.1.2 Harmful content.....	101
5.2 Defamation.....	109
5.3 Pornography.....	118
5.3.1 The Communications Decency Act, 1996.....	122
5.3.2 Indecent v. Obscene material .....	133
5.3.3 Maltese position on on-line pornography .....	140
5.4 Industry alternatives to censorship.....	147
<b>6. SOME PROCEDURAL ISSUES.....</b>	<b>151</b>
6.0 Introduction.....	151
6.1 Search and seizure.....	151
6.2 Interception .....	156
6.3 Encryption.....	159
<b>7. TRANSBORDER ISSUES.....</b>	<b>166</b>
7.0 Introduction.....	166
7.1 Jurisdiction.....	168
7.2 International co-operation.....	174
7.3 State sovereignty and transborder data flow .....	178
7.4 Harmonisation of substantive criminal law .....	180
<b>Bibliography.....</b>	<b>182</b>
<b>Index.....</b>	<b>189</b>