Data Security in Computer Networks and Legal Problems

Wolfgang Kilian/Andreas Wiebe (eds.)

stmv

S. Toeche-Mittler Verlag

Table of Contents

DATA SECURITY IN COMPUTER NETWORKS
AND LEGAL PROBLEMS (Kilian) 13

1. Computer Networks 13
2. Types of Data Transactions 13
   2.1. Financial Information 13
   2.2. Trade Accompanying Information 14
   2.3. Technical and Research Information 14
   2.4. Person-related Information 14
3. Assumed Threats concerning Computer Networks 14
   3.1. Deficiencies 14
   3.2. Misuse Complex 15
4. Required Basic Security Functions 15
5. Technical Standards and the Law 16
6. Technical and Legal Model of a Secure Computer Network 17
7. Levels of Regulations 18
   7.1. International Conventions and International Administrative Agreements 18
   7.2. Private International Contracts 18
   7.3. Law of the European Community 19
   7.4. National Law 19
   7.5. Private national contracts 19
8. Final Remark 20

TECHNICAL ASPECTS OF DATA SECURITY (Jandach) 21

1. Introduction 21
2. Theoretical Concepts of Data Security 22
   2.1. Data Protection Law 22
   2.2. "Orange Book" 23
   2.3. "Red Book" 24
   2.4. "Green Book" 24
      2.4.1. Discussion of the quality requirements 26
   2.5. "White Book" 26
2.6. Criteria of special user groups 27
3. Practical problems in the context of data security 27
   3.1. Security Problems in Connection with Stand Alone Computers 27
      3.1.1. Identification and authentication 28
         3.1.1.1. Single User Systems 28
         3.1.1.2. Multi User Systems 28
      3.1.2. Access rights 29
      3.1.3. Object reuse 29
   3.2. Practical Problems in Networks 29
      3.2.1. Network Security Problems in Relation to the ISO-OSI-Model 30
      3.2.2. Network-Commands 31
      3.2.3. Network security in general 31
   3.3. Cryptosystems and electronic signature 31
4. Closing remarks 32

OPEN SOCIETIES - CLOSED NETWORKS ? (Burkert) 33

1. Once A Perspective 33
2. Different Perspectives 33
3. Observations of Change 35
   3.1. The loss of tacit restrictions of information technology 35
      3.1.1 The Ethical Void 36
      3.1.2 Multiplication of risk factors 37
      3.1.3 Impossibility to contain the security debate 37
   3.2. The dialectics of security 37
      3.2.1. The Railway Traveller Syndrome 37
      3.2.2. The Broken Windows Syndrome 38
4. The Role of Law 38
   4.1. The functions of technology law 38
   4.2. The role of Criminal Law 39
   4.3. Re-Trusting Technology to Overcome Distrust 40
5. From Security to Control? 42

INTERNATIONAL AND NATIONAL LEGISLATION ON EDI (Martino/Palmerini) 45

1. The Electronic Document 45
2. The Levels of Legislation 47
   2.1. The International Legal Order 47
   2.2. National Legal Orders 48
3. International Instruments 48
   3.1. Model Interchange Agreements 50
4. National Legislation: The Situation in Europe 50
5. National Legislation: The Situation in Italy 52
   5.1. Positive Law 52
   5.2. The Law and Civil Procedure 52
   5.3 Evidence 53
   5.4 The Signature 53
   5.5. Electronic Data Interchange 54
   5.6. Case Law 55
   5.7. The Facsimile 55
   5.8. The EDIFORUM (Italy) Standard Agreement 55
6. Conclusion 56

EEC LAW AND POLICY IN TELECOMMUNICATIONS (Wiebe) 57

1. Introduction 57
   1.1. Telematics - technical and economic developments 57
   1.2. New Regulatory Problems in national telecommunications 58
   1.3. Demand for European action 59
2. EEC telecommunications policy and law 60
   2.1. Network infrastructure 61
   2.2. Services 63
      2.2.1. Competition directive 64
      2.2.2. ONP Directive 65
   2.3. Terminal equipment 68
   2.4. Standardisation 70
   2.5. Organisation 70
   2.6. EEC policies in adjacent fields 71
   2.7. Data Security 72
3. Complementary regulation on a case-by-case basis 73
   3.1. Competition law (Art. 85, 86) 74

3.2. Freedom to provide services (Art. 59) 77
3.3. Free Movement of Goods (Art. 30, 37) 77
4. Conclusion 78
Table of Community Documents in the Telecommunications Field 80

HOW TO ADVANCE COMPUTER SECURITY BY LEGAL INSTRUMENTS? (Kaspersen) 85

1. Introduction 85
2. Information Security 86
2.1. Policies 86
2.2. The levels of an Information Security Policy 86
3. Legal obligations 87
3.1. Examples in Present legislation 87
4. ITSEC, a case study 88
4.1. Who made it and what for? 88
4.2. How does ITSEC work? 89
4.3. Limitations of ITSEC 90
5. INFOSEC 91
6. Conclusions as to how Information Security can be advanced 91

LEGAL ASPECTS OF STANDARDIZATION AND CERTIFICATION OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS AN OVERVIEW (Stuurman) 95

1. Introduction 95
2. The process of standardization and certification 97
2.1. Standardization 97
2.1.1. Europe 97
2.1.2. Coordination 98
2.1.3. Other international organizations 99
2.1.4. Further players 99
2.2. Certification 100
3. Legal status of IT&T standards 102
4. Protection of standards documents and certification marks 103
4.1. Standards documents 103
4.2. Certification marks 105
5. Impact on liability 106
5.1. Damages 106
5.2. Standards and contractual liability 107
5.3. Product liability 108
5.4. General 109
6. Standardization and competition law 109
6.1. Effects on competition 110
6.2. The European Communities: unharmonized standards as a barrier to the internal market 110
6.3. De facto standards: the boundaries of cooperation and monopolies 113
7. Concluding remarks 114

EDI AND NATIONAL LEGISLATION (Riisnaes) 117

1. Introduction 117
2. What is security all about 117
2.1. More than just technical aspects 117
3. What kind of networks and data exchange are we talking about 118

3.1. EDI: definition 118
3.2. Internal networks like PC networks 118
3.3. EDI Closed Networks 119
3.4. EDI Open Networks 119
4. The duty to implement security measures 120
4.1. General security measures 120
4.2. Transmission errors 120
4.3. Data log 120
4.4. Certification 121
5. Other rights dependant on certain security measures 121
5.1. Transmission and Storage of Accounting Information 122
6. Acknowledgement of receipt 124
6.1. The duty to comply with a request for acknowledgement of receipt 124
6.2. What should be the consequences of failing to send such an acknowledgement? . 125
7. Evidential questions 126
7.1. Ensuring the admissibility of proof 126
7.2. Judgement of strength of proof 126
7.3. Regarding the burden of proof 126

DATA SECURITY AND FORMATION OF CONTRACTS (Elias) 129

1. Introduction 129
2. The risks and security procedures 129
3. Solutions adopted by law 130
4. To a new solution in an EDI-environment ? 131

THIRD PARTY SERVICES AND THE CONCEPT OF NEGOTIABILITY (Torvund) . 135

1. Basic third party services 135
2. Negotiability 136
3. Liability 137
4. Conflict of law 137
5. Conclusions 138

ELECTRONIC DOCUMENTS RELATED TO THE SWEDISH EDI-SYSTEM FOR CUSTOMS AUTHORITIES (Seipel) 139

1. Documents and related concepts 139
1.1. General viewpoints. Lexical definitions 139
1.2. Documents and legal language. An illustration – Swedish statutes 139
1.3. Characteristics of paper documents from a legal viewpoint 141
1.4. New kinds of documents: electronic media and messages 142
1.5. Characteristics of electronic data media and messages 143
2. Documents and the Swedish constitution. The right of access 146
2.1. Brief remarks on the development 146
2.2. Documents and recordings under valid law. Chapter 2 of the 146
2.3. Two doctrines: fixed documents and potential documents 147
2.4. Co-ordination with surrounding legislation: decision support, archives, data protection, criminal laws, etc. 149
2.5. A uniform document concept? 150
3. The Customs Data System (TDS) 150
3.1. Background. The development of the TDS. 150
3.2. Legal issues: an overview 153
3.3. Legal requirements, functional requirements and technical 154
3.4. The electronic seal 155

3.5. Electronic documents 156
3.6. Practical consequences and acceptance 157
4. Coordinated strategies and legal system management 158
4.1. Decisive factors for the development of concepts 158
4.2. Private solutions versus regulated and general solutions 158
4.3. A co-ordinated system of concepts and standards 158
4.4. The notion of legal system management 159
5. Concluding remarks. Research tasks 159
5.1. A legal theory of automated information handling 159
5.2. Law and informatics as the suitable framework 160

EDI MODEL AGREEMENTS (Seiler) 161

1. Present Extent of the Use of EDI 161
2. A Legal Framework for EDI 161
3. National EDI Model Agreements 162
4. The Necessity for EDI Agreements in Germany 165
5. The Relationship Between the EDI Agreement and the Commercial Contracts 166
6. Liability for EDI-Risks 167
7. The Electronic Message as Legal Evidence 170

INSURANCE COVERAGE AND EDI (Rettig/Otto) 173

1. Engineering and fidelity insurance 173
1.1. Insurable risks 173
1.2. Property damage 174
1.3. Financial loss 174
1.4. Summary 175
2. Third party liablity insurance 177
2.1. Bodily injury and property damage 177
2.2. Finacial loss 177
2.3. Exclusions 177
2.4. Legal defense 178
2.5. Coverage for pure financial losses 178

ABOUT THE AUTHORS 181