

Ot van Daalen

From Encryption to Quantum Computing

The Governance of Information Security
and Human Rights

ASSER PRESS

 Springer

Contents

1	Introduction	1
1.1	Introduction	1
1.2	Scope, Terminology and Limitations	4
1.3	Structure and Approach	6
1.4	Relevance of This Book	8
	References	11

Part I The Landscape

2	The Technological and Societal Landscape	15
2.1	Introduction	16
2.2	The Information Security Cycle	16
2.2.1	What Is Information Security?	17
2.2.2	Taking Information Security Measures	18
2.2.3	Three Generations of Hackers; from Mainframes, to PCs, to the Internet	19
2.2.4	The Life and Death of a Zero Day	22
2.2.5	The Devastating Effects of Exploits and Other Breaches	34
2.2.6	The Advantages of Exploits	38
2.3	The Encryption Landscape	39
2.3.1	Encryption Technologies as a Measure Against Unauthorised Access	40
2.3.2	The Difference Between Symmetric and Asymmetric Cryptography	41
2.3.3	The Adoption of Encryption Technologies	43
2.3.4	The Challenges for Governments to Access Encrypted Data	44
2.4	Quantum Computing: Crypto-killer App or Vapourware?	47
2.4.1	Quantum Mechanics	47

2.4.2	The Application of Quantum Mechanics to Perform Calculations	48
2.4.3	The Development of Quantum Computers	50
2.4.4	The Timeline for Developing a Quantum Computer that Can Break Encryption	53
2.4.5	The Impact of Quantum Computing on Encryption	55
2.4.6	Post-quantum Cryptography as a Mitigation Measure	59
2.4.7	The Development of Quantum Key Distribution as a Mitigation Measure	62
2.4.8	The Spin-Offs of the Quantum Race	63
2.4.9	Different Scenarios for Quantum Computing	64
2.5	Summing Up	65
	References	67
3	The Governance Landscape	85
3.1	Introduction	86
3.2	Governance of the Information Security Cycle	86
3.2.1	Regulation of the Measure-Taking Phase	87
3.2.2	Regulation of Security Research	98
3.2.3	Regulation of Unauthorised Access	104
3.2.4	Regulation of Unauthorised Interception	106
3.2.5	An Information Security Research Exception for Criminal Liability in Practice	107
3.2.6	Regulation of Disclosure, Exploits and Tools	108
3.2.7	Subconclusion	114
3.3	Governance of the Encryption Landscape	115
3.3.1	The First Crypto Wars	117
3.3.2	The Risks of Lawful and Unlawful Access	119
3.3.3	Regulatory Approaches in <i>Support</i> of Encryption	121
3.3.4	Regulatory Approaches <i>Restricting</i> Encryption	122
3.3.5	The Second Crypto Wars	125
3.3.6	Subconclusion	130
3.4	Governance of Quantum Computing	131
3.5	Summing Up	133
	References	134
 Part II The Human Rights Framework		
4	Human Rights in Context	151
4.1	Introduction	151
4.2	The Early Years of Human Rights	153
4.3	The Universal Declaration of Human Rights	154
4.4	Human Rights Protection in Europe	155
4.5	The Application of the Convention and the Charter	161

4.5.1	Interpretative Principles Under the Convention and the Charter	161
4.5.2	Interference, Foreseeability and Legitimate Aims	165
4.5.3	The Necessity Test	166
4.5.4	The Relevance of the Essence of a Right under the Charter	168
4.6	Different Typologies of States' Duties	169
	References	172
5	The Right to Privacy and Data Protection	177
5.1	Introduction	178
5.2	Concepts of Privacy	179
5.2.1	The Enlightenment	179
5.2.2	The Era of Mass Communications	180
5.2.3	The Introduction of Databases	181
5.2.4	The Introduction of the Internet	182
5.2.5	The Connection of Everyday Objects with a Computer Chip	183
5.2.6	The Values of Privacy	185
5.2.7	Summing Up	186
5.3	The Right to Privacy Under the Convention	187
5.3.1	The Scope of Private Life	187
5.3.2	The Scope of Correspondence	189
5.3.3	The Notion of Interference with the Right to Privacy Under the Convention	191
5.3.4	Negative Obligations Under Article 8 of the Convention	195
5.3.5	Positive Obligations Under Article 8 of the Convention	199
5.4	The Rights to Privacy and Data Protection Under the Charter ...	201
5.4.1	The Scope of the Right to Privacy and Data Protection	202
5.5	Conclusion	208
	References	210
6	The Right to Communications Freedom	217
6.1	Introduction	218
6.2	Three Perspectives on Communications Freedom	220
6.2.1	The Introduction of Print Technology	220
6.2.2	The Introduction of Communication Networks	222
6.2.3	The Era of Digitisation	224
6.2.4	Three Justifications for Protection of Communications Freedom	226
6.3	Communications Freedom and the Information Security Cycle	227

6.3.1	The Qualification of Interferences with Regard to Information Security Research	227
6.3.2	Proportionality of Restrictions on the Information Security Cycle	231
6.3.3	Duties and Responsibilities and the Information Security Cycle	235
6.3.4	Positive Obligations Flowing from the Right to Communications Freedom	237
6.3.5	The Right to Communications Freedom Under the Charter	238
6.4	Communications Freedom and the Application of Information Security	239
6.4.1	The Case Law Under Article 10 of the Convention	240
6.4.2	The Case Law Under Article 11 of the Charter	243
6.5	Conclusion	244
	References	246
7	The Right to Science	253
7.1	Introduction	253
7.2	Relevant Provisions	254
7.3	Interpretation of the Right to Science	256
7.3.1	Interpretation of the Right to Science Under the Covenant	256
7.3.2	Interpretation of the Right to Science Under the Charter	260
7.4	Relation Between the Right to Science and Communications Freedom	261
7.5	Limitations on the Right to Science	263
7.6	Conclusion: A Marriage of Science and Conscience	265
	References	266

Part III Synthesis

8	Human Rights-Compatible Information Security Cycle	
	Governance	273
8.1	Introduction	274
8.2	The Information Security Cycle Landscape	274
8.2.1	The Technological Landscape	274
8.2.2	The Governance Landscape	275
8.2.3	The Role of the State and of the EU in the Information Security Cycle	277
8.3	Human Rights Requirements for Information Security Cycle Governance	281
8.3.1	Strengthening Security Measures Protecting Human Rights	282

8.3.2	Weakening the Negative Impact on Human Rights of Security Measures	284
8.3.3	Promoting the Rights of Researchers in the Research and Disclosure Phase	286
8.4	Recommendations for Human Rights-Compatible Governance	288
8.4.1	Introduce Horizontal Governance of the Information Security Cycle	289
8.4.2	Promote Research and Disclosure of Vulnerabilities	292
8.4.3	Fix Vulnerabilities When They Are Found	295
8.4.4	Mandate a Manual Override	296
8.5	Topics for Further Research	298
	References	299
9	Human Rights-Compatible Encryption Governance	303
9.1	Introduction	304
9.2	The Encryption Landscape	305
9.2.1	Positioning this Book in the Broader Literature	305
9.2.2	Even with Good Governance, Security Breaches Remain	308
9.2.3	Encryption Technologies Restrict Unlawful Access	309
9.2.4	And Encryption Technologies Restrict Lawful Access	309
9.2.5	Encryption Makes Investigations More Difficult, Not Impossible	310
9.3	Human Rights Requirements for Encryption Governance	313
9.3.1	The Assessment of an Interference	314
9.3.2	The Assessment of Necessity	318
9.3.3	The Assessment of Proportionality	320
9.4	Recommendations for Human-Rights Compatible Governance	325
9.5	Topics for Further Research	326
	References	327
10	Human Rights-Compatible Quantum Computing Governance	331
10.1	Introduction	331
10.2	The Quantum Computing Landscape	332
10.3	Human Rights Requirements for Quantum Computing Governance	335
10.4	Recommendations for Human Rights-Compatible Governance	338
10.5	Topics for Further Research	341
	References	342

- 11 Summary and Conclusion 345**
 - 11.1 Introduction 346
 - 11.2 The Information Security Cycle 347
 - 11.3 The Human Rights Framework 348
 - 11.3.1 The Right to Privacy 349
 - 11.3.2 The Right to Communications Freedom 351
 - 11.3.3 The Right to Science 352
 - 11.4 Human Rights-Compatible Governance of the Information Security Cycle 353
 - 11.5 Human Rights-Compatible Governance of Encryption 356
 - 11.6 Human Rights-Compatible Governance of Quantum Computers 359
 - 11.7 Peering into the Future 362
 - 11.8 Making and Breaking with Science and Conscience 363
 - References 366