Information Technology and Law Series

Volume 38

Editor-in-Chief

Simone van der Hof, eLaw (Center for Law and Digital Technologies), Leiden University, Leiden, The Netherlands

Series Editors

Jef Ausloos, University of Amsterdam, Amsterdam, The Netherlands

Stephan Dreyer, Leibniz-Institut für Medienforschung, Hamburg, Germany

Gloria González Fuster, Law, Science, Technology & Society Studies (LSTS), Vrije Universiteit Brussel (VUB), Brussels, Belgium

Inge Graef, University of Tilburg, Tilburg, The Netherlands

Aleksandra Kuczerawy, Centre for IT and IP, KU Leuven, Leuven, Belgium

Eva Lievens, Faculty of Law, Law & Technology, Ghent University, Ghent, Belgium

Aurelia Tamò-Larrieux, Faculty of Law, Criminal Sciences and Public Administration, University of Lausanne, Switzerland, Switzerland

The *Information Technology & Law Series* was an initiative of IT *e* R, the national programme for information Technology and Law, which was a research programme set up by the Dutch government and The Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995 IT *e* R has published all of its research results in its own book series. In 2002 IT *e* R launched the present internationally orientated and English language *Information Technology & Law Series.* This well-established series deals with the implications of information technology for legal systems and institutions. Manuscripts and related correspondence can be sent to the Series' Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Ot van Daalen

From Encryption to Quantum Computing

The Governance of Information Security and Human Rights

ASSER PRESS

Springer

Ot van Daalen
Institute for Information Law (IViR)
University of Amsterdam
Amsterdam, The Netherlands

ISSN 1570-2782 ISSN 2215-1966 (electronic)
Information Technology and Law Series
ISBN 978-94-6265-634-5 ISBN 978-94-6265-635-2 (eBook)
https://doi.org/10.1007/978-94-6265-635-2

Published by T.M.C. ASSER PRESS, The Hague, The Netherlands www.asserpress.nl
Produced and distributed for T.M.C. ASSER PRESS by Springer-Verlag Berlin Heidelberg

The views expressed in this Yearbook are not necessarily those of the members of the Editorial Board, the Board of Recommendation and/or those institutions they represent, including the T.M.C. Asser Instituut and T.M.C. ASSER PRESS.

© T.M.C. ASSER PRESS and the author 2025
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording or otherwise, without written permission from the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

This T.M.C. ASSER PRESS imprint is published by the registered company Springer-Verlag GmbH, DE, part of Springer Nature.
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

If disposing of this product, please recycle the paper.

Acknowledgements

One added benefit of writing a book is getting a chance to acknowledge the family, colleagues and friends who make such an undertaking possible. I am deeply thankful to my parents—Rineke for reviewing the book in its various iterations and for nurturing my curiosity when I was young, and Bas, for his unfailing appreciation of my work, which made writing an extra pleasant task.

I am also deeply grateful to my supervisors, Joris, Mireille and—in the first half of this trajectory—Nico van Eijk. Joris, thank you for guiding me through this endeavor with gentle and clear guidance. Your input was invaluable, and I cherish our friendship. Mireille, your years-long experience and broad knowledge of the legal field has elevated this book to a level I couldn't have achieved without you. Nico, thank you for giving me the chance to do this project in the first place and for your supervision during the first half. And lastly, Harry Buhrman, thank you for entrusting this project with me—it has been a true privilege to work on this for the past years.

I am also very grateful to the people who shared their expertise with me. Jeroen van Beek, our regular cups of coffee were an important source of inspiration, and your detailed feedback on the security-related aspects of the book made it much better. Similarly, I am very grateful to Matthijs Koot and Jaap-Henk Hoepman for reviewing parts of my book. My gratitude also goes out to Brendan Newitt, for giving feedback the section on criminal law, and to Joran van Apeldoorn, for providing input on some of the quantum-related parts. Yvonne Donders, thank you for reviewing an early draft of the part of this book on encryption as part of the Ph.D. process. I am also indebted to the people who in interviews brought me up to speed on the topics discussed in this book: fukami, Rickey Gevers, Jeroen van der Ham, Christian van 't Hof, Bart Jacobs, Karst Koymans, Cees de Laat, Christian Schaffner and Aristoteles Tzafalias. As you will see, many of the points raised during those interviews are reflected in the book. My thanks also go out to the participants of the '19 workshop in Berkeley for providing feedback on an early draft of the encryption analysis, and to the participants of the '19 PLSC workshop on encryption policy and quantum technologies for providing inspiration on the issues developed in this book. This also goes for my quantum reading group—Geoff, Joran and Joris—for the discussions on all things quantum. And thanks to Erica Moore for editing part of my book and to

Melinda Rucz for helping with the research—you saved me a ton of work. Of course, all errors and omissions remain mine alone.

Let me also thank the wonderful colleagues and students at the IViR. I am truly privileged to work among such an excellent group of curious and kind people. In particular, thank you to those who stood in for me when I was finishing the book, and thank you to Margriet Pauws-Huisink and Anja Dobbelsteen for their help in the background.

This is also the place for a shout out to the b03k3nc7ub, Alexander, Maurits, Axel, Jeroen and Hans—I thoroughly enjoy our meetings and look forward to having many more of them. Hans, thank you for the feedback on my book and for helping me getting my technical infrastructure in order, and for the numerous times I typed in as I was writing this. Sjoera, thanks for kickstarting my career in digital rights, which ultimately led me to this book. Martijn, our working together in an early part of my career made a long-lasting impression and shaped my idea of excellence in work and life in general. My thanks also go out to my anonymous font-dealer, for providing feedback on the design and generally being there to help in various ways. And the same goes for my parents-in-law, Cees and Gisela de Groot, for their support. Thank you also to Michel for our monthly meetings, which I enjoy very much and helped me stay on track. And thank you to my sister Noor, for always being there for me.

Finally, I want to thank my wife Anne—for encouraging me in my decision to write this book, for enabling me to write it and for always supporting what I was doing. And thank you for your love, strength, integrity and kindness.

This book is based on my Ph.D., which is called “Making and Breaking with Science and Conscience: The human rights-compatibility of information security governance in the context of quantum computing and encryption”. I defended the Ph.D. in October 2022 at the University of Amsterdam. I also published parts of the Ph.D. (and thus this book) in separate papers.[1]The Ph.D. was supported by the Dutch Research Council (NWO) through the Gravitation-grant Quantum Software Consortium (no. 024.003.037).

January 2024 Amsterdam, The Netherlands

[1] Van Daalen O (2022) In Defense of Offense: Information Security Research under the Right to Science, Computer Law & Security Review 46: 105706; Van Daalen O (2023) The Right to Encryption: Privacy as Preventing Unlawful Access, Computer Law & Security Review 49:105804; Van Daalen O (2023) The Right to Root: Constructing a Claim to Control Devices from the Right to Privacy, JIPITEC, vol. 14, iss. 2023: 4, pp: 580-593; and Van Daalen O (2024) Developing a human-rights compatible governance framework for quantum computing, Research Directions: Quantum Technologies, vol. 2, 2024.

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 *Support* of Encryption 121
3.3.4 Regulatory Approaches *Restricting* 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