ASSER PRESS

Information Technology and Law Series | IT&LAW 38

From Encryption to Quantum Computing

The Governance of Information Security and Human Rights

Ot van Daalen

Springer

Information Technology and Law Series

Volume 38

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

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

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

Chapter 1
Introduction

Contents

Abstract This chapter explains the scope, relevance and structure of the research presented in this book. The scope of the research is on the application of the human rights to privacy (and data protection), to freedom of expression and to science, to the domains of information security, encryption and quantum computing. The analytical framework for this exercise understands information security as a continuous cycle of making and breaking, and the relationship between encryption and quantum computing as an example of this.

Keywords Privacy · Freedom of expression · Right to science · Information security · Quantum computing · Encryption

1.1 Introduction

If you squint, *everything* is information—and the rest are computers in disguise. Genes, guns, vaccines, viruses—all digitised, available at the click of a button. And what about cars, skyscrapers, fridges, bikes? They are basically elaborate structures built around silicon chips. One of the important questions of the twenty-first century then is: who gets to access and control these information and systems?

First, laws have an important role to play here. If you want to know what data your phone collects, you can invoke data protection rules. If someone steals your phone, you can go to the police to hopefully get it back. And if the police then wants to listen in on a suspect's conversation, the telecommunications company has to let them do so.

O. van Daalen, *From Encryption to Quantum Computing*, Information Technology and Law Series 38, https://doi.org/10.1007/978-94-6265-635-2_1

But organisational rules are also important. The telecommunications company requires its employees to keep information confidential. The police are likely to prohibit employees from sticking passwords to their screen. And the phone manufacturer might have policies in place to prevent intelligence agencies from introducing a backdoor in their software.

And finally, technology is important. The software on your phone limits what you can do with it. You can change the settings on your phone to prevent a thief from viewing you pictures. And although telecommunication companies may have to grant access to the police, they also take technical measures to protect their network from attacks by others.

Determining who can gain access and control is an important part, perhaps even the main function, of the field of information security. This is done by *taking* measures. An organisation can, for example, install a firewall to determine which information may enter, and which may leave the network. Or it can implement access management measures to control who gets to use a system. But these measures are also constantly under attack. From criminals to corporations, from governments to academics, it looks like everyone is trying to *break* all the things, all the time. This, too, is part of the field of information security.

In fact, an accurate description of information security would have to involve this continuous cycle of making and breaking. Decades ago, when computers were the size of rooms and their global number could be counted on two hands, users were already battling with administrators over who was allowed to gain access. As these machines have shrunk, multiplied and gained in importance, these battles remain, and their impact has greatly increased.

In response, states have in the past decades adopted rules on information security. Some require organisations to take information security measures. Some rules prohibit attackers from breaking these measures. And some rules are aimed at mitigation, for example obliging organisations to notify authorities of data breaches.

However well-intentioned most of these policies might be, when you look at them as a whole, they tend to focus on the *making* side of things, often at the neglect of the *breaking* side. This approach is incomplete. Software and hardware will continue to contain weaknesses, and people will continue to find and exploit them. This dynamic of making and breaking is inherent to information security and cannot be rooted out. In this book, building on best practices in information security, I call this process of making and breaking the *information security cycle*.[1] And I argue that, in order for policies in this domain to be compatible with human rights, those policies must be developed around this continual cycle of discovery and mitigation.

Now, this dynamic of making and breaking plays out in various fields of information security, but one domain in particular attracts the attention of governments: encryption technologies. This technology is a fundamental building block of many

[1] See for instance, Article 32(1)(d), which refers to a process of regularly evaluating and if necessary, updating security measures; the ISO/IEC 27001:2013 standard on information security management systems, in which a similar approach can be found, ISO, ISO/IEC 29147:2014—Information technology—Security techniques—Vulnerability disclosure, 15 February 2014; and the now-deprecated Guidelines on securing personal data of the Dutch Data Protection Authority, CBP 2013.

information security measures, because it allows users to restrict access to information and information systems. But this power to keep information confidential also poses an obstacle for governments, who have traditionally been able to gain access to the information they require in the course of investigations. In response, governments have over the past decades fought back to ensure they retain access, by subverting and regulating these technologies. Because encryption is such a foundational information security technology, the stakes in this technological-regulatory battle are high.

Another technological development, however, promises to raise the stakes in this particular cycle of making and breaking significantly: the development of quantum computers. These new kinds of computers, built with fundamentally different technologies from today's computers, may in the next decades provide enormous computing power to their users. And one of the potential applications of this power is to break a widely used form of encryption, public key encryption, something I'll explain further in this book.

These developments are not only highly relevant for policy—they also have an important human rights angle. First, this information security cycle of making and breaking is *itself* strongly related to human rights, leading to significant questions. For instance: to what extent is the work by information security researchers protected by the right to science and the right to communications freedom (a concept I explain further below)? And can you limit the development of quantum computers as such, to protect private communications?

But the issue of who gets access to information, and who gets to control information systems—in other words: the *application* of information security measures—is obviously also important to the enjoyment of human rights. Policies in this domain have a bearing in particular to the human rights to privacy, data protection and communications freedom. This perspective also leads to important questions. To what extent do governments have an obligation to limit unauthorised access to your private data? Or are they actually allowed to limit information security measures, in order to maintain access to your data when necessary? And what do human rights say about who gets to control your phone—to what extent can companies restrict the functionality of devices?

The relationship between information security and human rights has not been developed in depth in the literature yet, and especially not while viewing information security as this cycle of making and breaking (I discuss the most important books and articles below). In this book, I explore the relationship between human rights and this cycle of making and breaking, using the arms race between encryption technologies and quantum computing as an important case study. There is one aspect of this relationship that I am particularly interested in, namely the obligations of states under human rights instruments. This book thus centers around the following question: what constitutes human rights-compatible governance of the information security cycle, encryption technologies and quantum computing?

1.2 Scope, Terminology and Limitations

In answering this question, a number of restrictions apply. One important restriction lies in the way I look at the *function* of information security (and encryption and quantum computing), as well as *research* into these domains. I take what you could call an "information based" perspective: I am primarily interested in how governmental measures and technologies enable and restrict the flow of information, and—related to this—how these measures restrict the use of information systems. This is why I emphasise how information security measures impose conditions on the creation, distribution and use of information and discuss how the information security cycle is dependent on the possibility of researching and sharing information. This perspective was chosen because it fits well with the primary function of information security technologies, which is to channel information flows and restrict the use of systems (I will get to the concept of information security in Chap. 2, but this description suffices for now). It also fits well with the dominant function of science, which is to develop and share knowledge, which is a particular form of information.

Because of this "information based" perspective, this book is also restricted to three human rights: the rights to privacy (and data protection), to communications freedom and to science. These rights are for a large part about the extent to which governments may, or must restrict information flows. Other human rights are, of course, also relevant for determining what governments may and must do in these domains. These include the classical rights, such as the right to human dignity, to physical and mental integrity, to freedom of thought and to assembly. These also include economic and social rights, such as the right to just conditions of work (where information security measures may enforce unjust conditions) and the right to strike (which might be made more difficult by information security measures). In some contexts, these specific rights may be even more directly applicable than the rights to privacy, communications freedom and science. Where a state is, for instance, jamming encrypted communications of protesters, this would probably be evaluated primarily under the right to assembly, not the right to communications freedom. But the reasoning with regard to these human rights will roughly mirror the three human rights discussed in this book, in particular when it comes to the more classical human rights.

Territorially, governmental measures at the European Union (EU) level are the main focus of this book. Most of the issues surrounding information security are global in nature, and thus require at least a regional response. I further argue that the EU bloc can play an important role as a pioneer, setting a global standard for human rights-compatible governance in the domain of information security, similar to what it did with regard to data protection. In fact, as we will see, the EU is also already quite active in this domain. I occasionally discuss policies and practices in specific member states, to the extent that these are relevant for determining the scope of EU policy, for example because member states implemented the rules originating from the EU, because a national constitutional court issued a judgment which is relevant at an EU level or because enforcement often takes place at the national level. There

is of course an issue of competence here: many of these rules also affect national security, and national security falls within the remit of each member state. Moreover, to the extent that I conclude that states have a positive obligation to intervene, it is questionable whether this conclusion can be based on the Charter. I devote attention to these issues in Chap. 8.

This focus on the EU also means that I focus on the human rights instruments which are particularly relevant to EU and its member states, namely the European Convention of Human Rights (the Convention), the European Charter of Fundamental Rights of the European Union (the Charter) and the International Covenant on Social, Economic and Cultural Rights (the Covenant).[2] The Convention and the Charter play an important role for courts across Europe when assessing the compatibility of state measures. The Covenant, relevant for the right to science, is almost never applied in court, but it is generally considered to be an important source in policymaking, also in the EU.

From a substantive perspective, I discuss only a limited part of the broader field of information security: I focus on how information security technologies *restrict access* to information and *restrict control* of systems. But, as explained in Chap. 2, information security is about much more. For example, information security is also about the availability of information—whether a website is up or down—and about the authenticity of information—whether it has not been tampered with. However, assessing the connection between human rights and these other functions of information security would require a significantly different analysis, and is best suited for a different book.

In addition, information security is not only about technological measures in a narrow sense it is also about measures which are more organisational in nature, such as confidentiality obligations in contracts with employees, and organisational policies relating to access of systems. My analysis revolves around those aspects of information security which have a more technological character, such as encryption algorithms and changes to user software, because the policy debate is focused on these aspects. I will, however, occasionally also discuss the organisational framework in which these measures are embedded.

Part of this book is about developing a framework for substantive policy in the domain of information security. Throughout the book, I group governmental policies and practices under the header of *governance*, a term many will associate with a broader meaning, encompassing public and private institutions as much as rules.[3] I thus discuss only a part of what falls under the broader header of *governance*—*substantive governance*, if you will. This means I also leave a lot of things out

[2] Council of Europe (1950) European Convention on Human Rights (as amended by Protocols Nos. 11 and 14 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16); European Union (2009) Charter of Fundamental Rights of the European Union; United Nations (1976) International Covenant on Economic, Social and Cultural Rights.

[3] See for example Möllers 2006. Under one oft-cited definition, this is the manner in which power is exercised in the management of a country's economic and social resources for development; The World Bank 1994, p. vii. This includes topics such as transparency surrounding policymaking, accountability of executive power, and the strength of civil society.

which are especially relevant in the context of information security. In particular, I barely touch on the administrative aspects of institutions which are tasked with safeguarding information security. For instance, I do not discuss the powers which are accorded to national cybersecurity centers and intelligence agencies, the role of public-private initiatives and how tasks are divided between these bodies. I also do not discuss in depth the role of the private sector in information security, for example through standardisation and market power. I acknowledge that these play a significant role in shaping the information security landscape, also historically. The reason for restricting my research this way has to do with space and clarity: the book already touches on a broad ranges of topics and including these aspects would not be helpful for the analysis. Connecting these aspects to human rights is, however, a valuable topic for further research.

Following up on this theme: in writing about substantive policy, I often refer to the *government* or *state* as if it were a monolithical unit. I acknowledge that things are usually not that simple. There are various institutions within a government, with often conflicting interests, and there sometimes are also competing teams within one institution. For example, intelligence agencies have already for a long time had the conflicting tasks of securing communication of some, while intercepting communication of others. This also explains why governance sometimes is inconsistent or illogical. Still, human rights law is not really concerned with the explanations as to *why* governance is the way it is—courts when applying human rights instruments view the state as the main unit of policy making, and I will do the same.

1.3 Structure and Approach

In answering what constitutes human rights-compatible governance of the information security cycle, encryption technologies and quantum computing, I employ a simple structure, distinguishing between the facts, the rules and the application of those rules. This book thus consists of three main parts. In Part I, I answer the question how governments are, and could be shaping the domains of information security, encryption and quantum computing. Because I review the human rights-compatibility of governance measures, the "facts" in this case not only consist of the technological landscape, but also the legal framework shaping this technological landscape. In Part II, I then discuss the rules by which these governance measures need to be assessed: this is the human rights framework which imposes limits on what governments *may* do and provides obligations on what governments *should* do. And then in Part III, I apply this human rights framework to each of the domains of information security, encryption technologies and quantum computing.

Zooming in on each of the chapters, the structure is as follows. In, on the technological landscape, I first describe the continuous cycle of making and breaking ingrained in information security—the information security cycle. I also discuss how encryption technologies are an important information security measure and explore how broad adoption of these technologies potentially impedes access to information

by governments. I then discuss how quantum computing works, how this technology can break encryption and how these technologies can be expected to develop in the future.

In Chap. 3, on the legal landscape, I then provide an overview of current and potential governance measures in these domains. Here, I investigate how governmental policies and practices impact the information security cycle, again also focusing on encryption and quantum computing. I do this by discussing what the rules are, whether these rules are enforced, and whether uncertainty on the rules and their enforcement may make people more fearful to do things which would actually be legal or not enforced. I also explore how governments may steer future development through a broad range of potential interventions, for example by giving grants, investing in education and providing information on security threats. The goal is not to be complete—rather it is to provide an analysis of the most important governance approaches in these domains and illustrate the interests at play.

This chapter is partly a mere description of the rules. It is, however, also an analysis of *gaps* in regulation, particularly when it comes to information security. I conclude in the synthesis that states have an obligation under the human rights to privacy and communications freedom to close gaps in the information security cycle, so it is important to understand what these gaps are. For this gap analysis, I take as a starting point that many of the regulations discussed in this chapter are aimed at strengthening information security measures. And where these rules fail to do so in practice, I consider this a gap. My analysis is further based on the assumption that a smooth-functioning feedback loop in finding and fixing vulnerabilities is important for strengthening information security measures. Where this feedback loop is not functioning well, I also consider this a gap. To be clear: whether a gap needs fixing in view of human rights requirements is not part of this chapter—those questions will be discussed in the third part of this book.

After having described the landscape in Part I, I then develop the normative framework in Chaps. 4, 5, 6 and 7. As noted above, the yardstick by which I measure governmental policies and practices is human rights law, in particular the right to privacy (and data protection), the right to communications freedom (a term I explain further in Chap. 6), and the right to science. For the rights to privacy, data protection and communications freedom, I apply the Convention and the Charter. I only discuss national law when it is relevant for furthering the understanding of similar concepts as laid down in these European instruments. For the right to science, the Covenant and the Charter are relevant. In Chap. 5, I then discuss the rights to privacy and data protection under the Convention and the Charter. In Chap. 6, I review the right to communications freedom under these instruments. And in Chap. 7, I explore the right to science under the Covenant.

Finally, in Chaps. 8–11, I apply the human rights framework to the landscape described in Part II. For each chapter, I mirror the structure employed throughout this book—first laying out the factual and legal considerations for a specific domain, then summarising the conclusions with regard to human rights in this domain, and then developing policy recommendations. These chapters build on what has already been said in the earlier parts of the book—the sources are thus limited, while some of

the earlier conclusions are reiterated. But the emphasis lies on the conceptual insights: what do the particular human rights imply for human rights-compatible governance in each domain. For each chapter, I also mention topics for further research. The book will end with the conclusion in Chap. 11, summarising my main findings.

I have frozen the description of the technological landscape, governance developments and analysis of case law around the beginning of 2023, and have incorporated only major developments in these fields afterwards.

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. Parts of the Ph.D. (and thus this book) were published in separate papers.[4]

1.4 Relevance of This Book

The most important contribution of this book lies in the in-depth analysis of information security from the perspective of human rights. Academics have paid little attention to human rights in the context of information security, let alone understanding it as a dynamic process. Burkart and McCourt performed a somewhat similar analysis in *Why hackers win: power and disruption in the network society*, but this is focused more on the US, with less attention devoted to legal aspects.[5] Dizon, in his book called *Breaking and Remaking Law & Technology*, describes information security governance but does not pay as much attention to human rights as well.[6] Porcedda's book on the relation between "cybersecurity" and the right to privacy and data protection also deserves to be mentioned, but it has a narrower focus and a different goal, namely resolving the apparent tension between privacy and cybersecurity.[7] Arnbak in his 2015 book also touches on information security and human rights, but focuses more on an analysis of the development of different policy instruments in this field.[8] This focus on human rights also sets my book apart from currently dominant approaches to research in the field of information security, which are mostly about the economics, psychology and technology of information security.[9] For completeness, there have been some articles on the concept of *human security*, opposing it with *cybersecurity*,

[4] Van Daalen 2022, 2023 and two forthcoming papers, one on digital autonomy and the right to privacy, and one on quantum computing policy.

[5] Burkart and McCourt 2019.

[6] Dizon 2016.

[7] Porcedda 2017.

[8] Arnbak 2016.

[9] See Anderson 2020, Chap. 3 (psychology), Chap. 8 (economics) and referenced literature; see for an analysis of vulnerability disclosure policy from an economics perspective ENISA.

but this concept could be more grounded in human rights law.[10] And while human rights do play an important role in the context of encryption technologies, there is no recent literature analysing how encryption regulations should be assessed under European human rights law: the last in depth analysis, by Schulz and Van Hoboken, stems from 2016.[11] Finally, there is very little analysis of the legal implications of quantum computing, let alone of the human rights aspects of quantum computing. The major work in this field is *Law and Policy for the Quantum Age* of Hoofnagle and Garfinkel, but it has a decidedly US slant and touches on human rights issues only tangentially.[12]

In this book, I take the cycle of making and breaking as a central point in my analysis. While information security experts indeed view their work as part of this cycle, this generally is not how governance in the field of information security is devise. Dizon, mentioned above, also explores how the law affects the work of security experts, but does not emphasise the cyclical nature of information security itself. I believe that focusing on the offensive and defensive side of information security equally provides new insights as to how policy in the domain of information security—as well as in the domains of encryption and quantum computing—should be devised. It means, for example, that you need to actively provide room in governance for doing research on how to break things. This approach also emphasises the risk mitigation aspects that are involved when exercising human rights: if you know that vulnerabilities will continue to be found, it makes more sense to focus on mitigating the risks when they are found, then on finding them in the first place.

Another contribution of this book, is that I provide an up-to-date overview of EU governance measures in the domains of information security, encryption and quantum computing, taking the cyclical nature of information security as a starting point. Parts of these measures have already been mapped separately. See in particular, Arnbak's analysis of information security policy in the context of data protection, telecommunications, digital signatures and certificates, cybercrime and critical infrastructure, and Hofman's analysis of security measures in the context of data protection (see further the sources in Chap. 3).[13] There are furthermore many overviews of encryption governance, but this study provides a relevant contribution by discussing some of the more recent proposals from a human rights perspective and further developing the positive obligations of states in this regard. And when it comes to quantum computers, this is the first book which provides an overview on the limited governance measures in this domain in the EU (Hoofnagle and Garfinkel in their book mentioned above only touch on this in passing).[14]

---

[10] See for example Cavelty 2014; see also Salminen and Hossain 2018.

[11] Schulz and van Hoboken 2016.

[12] Hoofnagle and Garfinkel 2021.

[13] Arnbak 2016; Hofman 2022.

[14] Hoofnagle and Garfinkel 2021. Some papers have been written outlining a broad vision on governance of quantum computing, but there is no comprehensive attempt yet to map this governance space; see Perrier 2021; Johnson 2019; de Wolf R (2012) What Quantum Computing Can Do for You. Inaugural lecture; de Wolf 2017.

This broad mapping of governance measures also allows for a comprehensive gap analysis, resulting in a number of important insights. First, an insight from this analysis is that information security governance measures should be applied across all systems which are vulnerable to attacks—something which is not currently the case. This has already been suggested by BEUC in 2019, but without a legal analysis.[15] Also, the introduction of the *attack surface* as an atomic unit for policymaking is new: from an information security perspective, this is where the action takes place, so this is where governance measures should be directed. This has not been proposed previously. Lastly, my suggestion to introduce an exception for information security research has been proposed in other places before, but in this book I also provide the legal backing for this, basing it on the right to science and the right to communications freedom.[16]

On the human rights side, an important analytical tool developed in this book is the focus on the risk of *unlawful access*. Human rights courts have in the past emphasised the safeguards for *lawful access* to interests protected by privacy and communications freedom, mostly disregarding states' obligations when it comes the other type of access, *unlawful access*. But in fact, information security measures are mostly about preventing unlawful access. My conclusion is that measures which significantly increase the risk of unlawful access to information or systems, or unlawful control of information and systems, should be considered an interference. Furthermore, the conclusion that in many cases this interference is disproportionate, given the current state of information security, is important in future analyses of states' obligations in this domain.

With this book, I also draw attention to the double-edged nature of information security measures for human rights. Information security measures may in certain instances protect human rights, when the *human in question* is in control of the application of the measures, or when they benefit from this application. You might be able to determine yourself when you want to apply strong encryption, or strong encryption is built in the device you're using by default: in both cases you benefit from the privacy-protecting properties of encryption. But these measures may also negatively impact human rights, by restricting the freedom of people to access information and use systems. This perspective is already important for the analysis of the relationship between information security and human rights.

My analysis of the right to science also provides useful insights. The most relevant conclusion is that the duty of care that comes with the right to science has a role to play in steering policy debates. This duty of care under the right to science implies that policymakers and researchers have an obligation to mitigate the risks of potentially dangerous technologies. For information security, this means that the right to science also imposes on researchers a duty to disclose their findings. This is completely new and has not been proposed in literature before (it also leads to a number of practical questions on the boundaries of this duty). For quantum computing, the implication

[15] Oliveira da Silva 2019.

[16] See for example Schaake et al. 2018; ENISA (2015), para 6.3; and ENISA (2013), p. 10.

that governments must on the basis of human rights obligations invest in alternative, quantum resistant technologies, is also an important insight.

Now, although I limit myself mostly to information security in this book, the conclusions on states' obligations with regard to the right to science do not remain limited to information security only. These can also be translated to other fields where research can have positive or negative impacts.[17] For example, advances in artificial intelligence technologies can be used to impersonate people, but also to detect fake news. Virology research can be used to make viruses more deadly, but also to make vaccines. Understanding these technologies as part of a cycle makes it possible to develop governance steering their development and use in the public interest. In particular, the emphasis in information security on risk mitigation can also be useful for other fields—it could imply that experimenting with viruses can only be allowed if vaccines are developed simultaneously. I touch on this question in the conclusion.

References

Articles, Books and Other Documents

Anderson R (2020) Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd edn. John Wiley and Sons, Indianapolis.

Arnbak AM (2016) Securing Private Communications: Protecting Private Communications Security in EU Law: Fundamental Rights, Functional Value Chains, and Market Incentives. Kluwer Law International, Alphen aan den Rijn, The Netherlands.

Burkart PC, McCourt TM (2019) Why Hackers Win: Power and Disruption in the Network Society. University of California Press, Oakland.

Cavelty MD (2014) Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Science and Engineering Ethics 20:701–715. https://doi.org/10.1007/s11948-014-9551-y

CBP (2013) Richtsnoeren: Beveiliging van persoonsgegevens. https://www.autoriteitpersoonsgegevens.nl/uploads/imported/beleidsregels_beveiliging_van_persoonsgegevens.pdf. Accessed 14 December 2023.

de Wolf R (2017) The Potential Impact of Quantum Computers on Society. arXiv:171205380 [quant-ph].

Dizon MAC (2016) Breaking & Remaking Law and Technology: A Socio-Techno-Legal Study of Hacking. Tilburg University, Tilburg.

ENISA (2013) The Directive on Attacks against Information Systems: A Good Practice Collection for CERTs on the Directive on Attacks against Information Systems. https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems. Accessed 14 December 2023.

ENISA (2015) Good Practice Guide on Vulnerability Disclosure: From Challenges to Recommendations. https://www.enisa.europa.eu/publications/vulnerability-disclosure/at_download/fullReport. Accessed 14 December 2023.

ENISA (2018) Economics of Vulnerability Disclosure. https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure. Accessed 14 December 2023.

[17] See on the governance of other types of dual-use technologies Harris 2016, comparing nuclear and biological technologies with the governance of vulnerabilities in cyberweapons.

Harris ED (ed) (2016) Governance of Dual-Use Technologies: Theory and Practice. American Academy of Arts & Sciences. https://www.amacad.org/publication/governance-dual-use-technologies-theory-and-practice/section/7. Accessed 14 December 2023.

Hofman JA (2022) De beveiliging van persoonsgegevens: Over de juridische invulling van art. 5 lid 1 onder f en 32 AVG. Kluwer Juridische Uitgevers, Deventer.

Hoofnagle CJ, Garfinkel S (2021) Law and Policy for the Quantum Age, 1st edn. Cambridge University Press, New York.

ISO, *ISO/IEC 29147:2014 - Information technology - Security techniques - Vulnerability disclosure*, February 15, 2014.

Johnson WG (2019) Governance Tools for the Second Quantum Revolution. Jurimetrics 59:4.

Möllers C (2006) European Governance: Meaning and Value of a Concept. Common Market Law Review 43: 313–336.

Oliveira da Silva F (2019) Keeping Consumers Secure. How to Tackle Cybersecurity Threats through EU Law, BEUC-X-2019-066. https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-066_keeping_consumers_secure_-_how_to_tackle_cybersecurity_threats_through_eu_law.pdf. Accessed 14 December 2023.

Perrier E (2021) Ethical Quantum Computing: A Roadmap. arXiv:210200759 [quant-ph].

Porcedda MG (2017) Cybersecurity and Privacy Rights in EU Law: Moving beyond the Trade-off Model to Appraise the Role of Technology. European University Institute.

Salminen M, Hossain K (2018) Digitalisation and Human Security Dimensions in Cybersecurity: An Appraisal for the European High North. Polar Record 54:108–118. https://doi.org/10.1017/S0032247418000268

Schaake M, Pupillo L, Ferreira A, Varisco G (2018) Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/. Accessed 14 December 2023

Schulz W, van Hoboken J (2016) Human Rights and Encryption. UNESCO.

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.

The World Bank (1994) Governance: The World Bank's Experience. The International Bank for Reconstruction and Development/World Bank, Washington, DC. https://elibrary.worldbank.org/doi/abs/10.1596/0-8213-2804-2, Accessed 3 January 2024.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Part I
The Landscape

Chapter 2
The Technological and Societal Landscape

Contents

Abstract This chapter explores the technological landscape, focusing on three topics: information security, encryption and quantum computing. With regard to information security, it highlights the ongoing struggle between creating secure systems and finding their weaknesses. It further underlines that the current state of information security is notably poor, with the complexity of IT systems providing ample opportunities for attackers. The chapter also touches on the dilemma faced by researchers who discover vulnerabilities on how to responsible disclose their findings. It finally examines the relationship between encryption technologies and quantum computing, suggesting that the development of quantum-resistant technologies is

O. van Daalen, *From Encryption to Quantum Computing*, Information Technology and Law Series 38, https://doi.org/10.1007/978-94-6265-635-2_2

crucial. The discussion intertwines technology and human rights, seeking a balance between government access to encrypted information and protecting individual rights.

Keywords Information security · Encryption · Quantum computing · Vulnerabilities · Coordinated vulnerability disclosure

2.1 Introduction

To most legislators, information security is something you *have*, not something you *do*. Your computer is either secure, or it is not, and when it is not—well, that's a problem. Politicians and victims often respond by assigning blame—the hacker who entered the system did so unlawfully, or the company left a gaping hole in its server because it did not patch it in time. But if we take a step back, it is clear that this unpatched server was not the first in the history of computing—millions have come before it, and millions will follow. What we see instead is a recurring process of finding weaknesses and fixing them, only for the next weakness to be discovered and fixed, and so on. That cat-and-mouse game between offence and defence? *That is* information security.

In this chapter, I take look at this continuous process, which I call the information security cycle.[1] In the first section, I describe the cycle itself. Then I describe an important measure which many organisations use to protect themselves: encryption technologies. In the final section, I review a technology which is expected to undermine many of these encryption technologies: quantum computing.

2.2 The Information Security Cycle

A central point of this book is that for policymaking, information security should be considered to be a continuous process. In this section, we look at this feedback loop from various vantage points. We first take the perspective of an organisation that wants to defend itself through its information security policy. Then we zoom out and take the perspective of a historian, showing how the cycle of making and breaking is ingrained in the user culture associated with different generations of computers, from mainframes in the seventies to current cloud services. Next, we take a deep dive into the life of a vulnerability, from initial discovery to final fix. And we acquaint ourselves with the work of those on the bug-hunting trail, from intelligence services to criminals, from companies to academic researchers. Lastly, we look through the eyes of the user and consider the devastating effects that the exploitation of a vulnerability

[1] Parts of this chapter have already been published in Van Daalen 2022, 2023a, 2023b, 2024.

can have on people's lives, and on IT infrastructure, but we also touch on some of the positive aspects of weaknesses in information security systems.

2.2.1 What Is Information Security?

This book is about information security—but what *is* information security exactly? In the literature, information security is often framed in terms of desirable *security properties* (also called *security objectives*). Three properties are commonly seen as fundamental building blocks: *confidentiality* (preventing unauthorised access to information), *integrity* (preventing unauthorised alteration of information) and *availability* (ensuring that information remains accessible to authorised users), often abbreviated as the CIA-triad.[2] There is an ongoing debate about whether other security properties should also be regarded as fundamental, or whether they are merely a combination of lower-level functions. For example, some authors include *authentication* (identifying an originating entity or the origin of data) and *non repudiation* (preventing the denial of previous commitments or actions) under this header as well.[3]

It is not necessary to resolve this debate here—all these security properties are just building blocks. For this book, a more interesting question is: what do you *use* those properties for? In this book, I am focusing on a particular function of information security—the function of (i) *access* and (ii) *control*, to and of, (iii) *information* and (iv) *systems*. Let me explain these four aspects. First, when I say information security is about restricting *access* to information, I am primarily talking about the building block of *confidentiality* described above. And then secondly, I'm broadening this notion of access to also include access to *systems*—to your phone, your computer, to your account, etc. Third, when I say *control* of information, I am talking about ways in which the use or distribution of this information can be restricted—this, for instance, is what digital rights management measures are aimed at. Obviously, information security plays an important role in those settings as well. And finally, when I talk about control of *systems*, I mean how information security measures can be aimed at restricting their functionality—think of an e-bike with a digitally imposed maximum speed.

To be clear: information security is about more than this. For example, I'm not touching on the function of information security for ensuring trust. But for this book, this limited notion of information security as access and control, to and of, information and systems, plays an important role in my analysis in subsequent chapters.

There is also another aspect to the notion of information security which is worth discussing upfront—*whose* information security are we talking about? When Apple takes information security measures to restrict users from installing apps outside of

[2] See Arnbak 2016, Chap. 5 for an in depth discussion of these concepts; and Menezes et al. 1997, p. 4 for the definition of the first two.

[3] Menezes et al. 1997, p. 4; see also Arnbak 2016, Chap. 5.

the app store, you could argue that this is done to keep the user secure: this way you can prevent malicious apps from being installed on the phone. But it also limits the user in what it can do with the phone. In fact, perhaps this measure benefits Apple even more than it benefits the user—Apple can ensure that it takes a cut of the income from all apps which are installed on this phone and exclude apps which compete with its own apps. We often see that the organisations which take information security measures consider the user to be an adversary—and this has implications for human rights as well.

This notion of who is the beneficiary of an information security measure is also relevant for a final distinction I want to discuss at the outset: the difference between information security and cybersecurity. Unfortunately, there is no clear line between the two. For one, cybersecurity is a buzzword, sometimes used to attract the readers' attention or to frame an old topic in a new way. It's also a vague term. As a result, you will sometimes see the term *cybersecurity* used in a way which is similar to my description of *information security* above. More often, though, the term *cybersecurity* is used to refer to a particular application of information security, namely to further specific, mostly state-related interests.[4] In those cases, it's about protecting critical infrastructure, about protecting against online terrorism, about online attacks by nation states, etc. And it can also be used in a context where it is more focused on preventing crime, gaining access to encrypted data in an investigation, even about preventing the stealing of intellectual property. For this book, however, it is not so important to delineate the two exactly, because I will avoid the term altogether, precisely because it has no clear meaning.

2.2.2 Taking Information Security Measures

Now, many organisations will, at some point in their development, take information security measures to defend against attacks. But it can be difficult to determine which measures make the most sense. Over the past decades, standard practices have emerged to help organisations make the best choices, even in the face of changing circumstances. These are generally subsumed under the *plan-do-check-act* cycle, originally developed for quality assurance in manufacturing, but applied in other contexts since, including in information security.[5]

In the first phase of the cycle, the *plan*-phase, an organisation will decide which measures are necessary in view of the risks. These decisions are usually laid out in an information security policy. In this policy, the *security requirements* (e.g. that certain information must remain confidential) are described in view of the *risks* to certain

[4] See Nissenbaum 2005.

[5] In the GDPR, controllers and processors are required to implement "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing", Article 32(1)(d); in the ISO/IEC 27001:2013 standard on information security management systems, a similar approach can be found; see also the now-deprecated Guidelines on securing personal data of the Dutch Data Protection Authority; CBP 2013.