SMART CITY GOVERNANCE

ELSEVIER

ALOIS PAULIN

SMART CITY GOVERNANCE

This page intentionally left blank

SMART CITY GOVERNANCE

Alois Paulin
Institute of Informatics
Faculty of Organisation Studies
Novo mesto
Slovenia

ELSEVIER

Elsevier
Radarweg 29, PO Box 211, 1000 AE Amsterdam, Netherlands
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-816224-8

For information on all Elsevier publications
visit our website at https://www.elsevier.com/books-and-journals

Publisher: Joe Hayton
Acquisition Editor: Brian Romer
Editorial Project Manager: Andrae Akeh
Production Project Manager: Anitha Sivaraj
Cover Designer: Greg Harris

Typeset by SPi Global, India

CONTENTS

This page intentionally left blank

ACKNOWLEDGMENTS

Many years of work, study, and thinking lie behind the ideas and insights presented in this book—these are solitary activities, which one can do alone. But this book would not be if it weren't for the support of others who provided me with their directions, inspiration, time, and patience.

I owe the deepest gratitude to my father. The life he offered me and the path he set me on from childhood are truly unique. He sacrificed his life for the benefit of his children, and without this, I would not have had the means to realize this project. His struggle to regain and preserve our ancestors' fortune later became mine, providing me with the deepest insight into how systems of power operate. Ultimately, it was these struggles that inspired me in the explorations and research that culminated in this book. To this end, this book is also a deep bow to my lineage, to the achievements of my ancestors, and to the sufferings they had to endure.

This book would not exist without the inspiration and persistence of Sahar Sahebdivan. She was my muse—she opened my eyes so that I could see the world. Thanks to her, the perspectives that I am able to assume are of unique deepness, clarity, and sophistication. The struggles she and her own ancestry endured helped me see beyond the narrow confines of the culture I was born into. Sahar helped me preserve hope in the virtue of science despite the numerous insecurities that pester our generation. I dedicate this book to her in deep love and admiration.

Was it not for the critique, guidance, and discussion provided by numerous colleagues from academia, I could never have composed a piece as involved as this. Among my many colleagues, I owe a special thanks to Klaus Lenk, who shared his knowledge and views on the applicability of technology in the context of governance with me. Was it not for the many debates with him and the abundance of invaluable literature he provided me with, I might have missed the forest through the trees.

Thanks to Karishma Hathlia, who spent countless hours on making this book clear to read and patiently brought the words, sentences, and paragraphs in their right order. Her insistent fights both with the text and me helped significantly in bringing out the ideas presented in this book with a clarity that would not be possible without her help.

Last but not least, I must thank my former colleagues from the Computer Vision Lab at Vienna University of Technology for their patience and generous hosting during my years of research and writing, and my colleagues from the Faculty of Organization Studies in Novo mesto for their support that helped me complete this episode of my life in style.

QUOTE

Sir Humphrey: "If the right people don't have power, you know what happens? The wrong people get it: politicians, councilors, ordinary voters."

Sir Woolley: "But aren't they supposed to in a democracy?"

Sir Humphrey: "This is a British democracy! British democracy recognizes that you need a system to protect the important things of life and keep them out of the hands of the barbarians—things like the opera, Radio 3, the countryside, the law, the universities—both of them. And we are that system. We run a civilized, aristocratic government machine, tempered by occasioned general elections. Since 1832 we have been gradually excluding the voter from the government. Now, we got them to a point where they vote just once every five years for which bunch of baboons will interfere with our policies, and you are happy to see all that thrown away?"

"Power to the People"[1]

[1]Jay, A., Lynn, J., Lotterby, S., 1988. Power to the People. Yes Prime Minister.

This page intentionally left blank

INTRODUCTION

The "smart city," while originally no more than a marketing term, today refers to a broad set of concepts, business and marketing trends, and research toward transformations in governance and economy. Specifically, the smart city idea focuses on the modern urban space from a perspective of "smart" technologies. To this end, the applicability and/or application of "smart" technology is researched in various domains such as water and energy supply, transportation, health care, emergency services, tourism, waste management, construction, government, and commerce. What these domains have in common is nothing less and nothing more than that they influence how attractive a city is for individuals and businesses to settle in. The importance of these domains for the prosperity of the common good makes them matters of public importance and as such subjects them to public governance. In other words, this means that municipal authorities and politicians strive to make their city a better, safer, and kinder place to live and work in.

The "smart" in smart city is then a similar "smart" to that in "smartphone" and as such refers to the use of advanced technologies in making the city better in many dimensions. Common approaches in making the city smarter are the implementation of various digital services, such as the online provisioning of information for tourists and locals, online services for navigating the public transport system and ticketing, digitalized administrative services for online interaction with city government, telemetric systems applied in energy and water supply, and systems for traffic management. This way, city governments try to do what is within their means, to turn their city into a "smart" city by means of digitalizing and computerizing its infrastructure and services.

Several books to advise city governments on how to make their city "smart" have been written. Anthopoulos' (2017) *Understanding Smart Cities* provides a good overview of the state of the art, both in theory and practice, in this regard. This book, however, has different objectives. It follows the question of how smart city governance can be *informatized*—that is, how the city governments, providers of communal services, and other agents that have official power in making the city a better place can be controlled and steered by means of information technology from within cyberspace.

This question is novel. Public governance has always been a matter of institutions controlling individuals or other institutions, that is, humans in the respective position of power controlling (or at least aiming to do so) other humans or institutions. But over the past couple of decades, circumstances have changed radically.

The invention and engineering of the Internet and other electronic messaging technologies throughout the 1960s–80s created a solid infrastructure for remote communication of all types of digital data. This infrastructure is unprecedented and unique—a giant technological leap in available tools and possibilities. The unifying infrastructure of the Internet has enabled the modern *cyberspace* to emerge as a new dimension for interaction through space and time. The *cyberspace*, then, gave rise to the *digital era*, a novel epoch in human history in which interaction became possible in ways that were never possible before. The unprecedented spread and development of Web technologies in the 1990s and throughout the first decade of the new millennium further extended the outreach of end-user-oriented ICT to a state of ubiquity. Fully fledged mobile computers assume the role of always-online phones, cameras, Web terminals, data servers, cryptodevices, etc. The ever-present availability of ICT has enabled the rise of advanced services, which facilitate the transaction of goods and services, the virtualization and digitalization of services, the informatization of credit transfer, etc.

We are now in the second decade of the new millennium and generations that grew up in the 1980s–90s and later do not perceive the cyberspace as a special set of tools and technology, but rather as an integral part of their reality. In this reality, new ways of conduct are possible, which has allowed civilization to evolve to a new level. In the last few decades, we experienced a revolutionary change in how communication, transportation, and navigation take place; how ordering and shipping of goods are conducted; how research is done; how information is conveyed; and so on. Thus, for example, booking airplane tickets to cities on the other side of the world, booking a hotel there, planning public transport for getting from the airport to the hotel and to navigate through town, getting advice on how to avoid scams and hazards in faraway destinations, and purchasing goods and services there have all been made incredibly simple through ICT—to such an extent that it is easier and less time-consuming to plan a trip from Vienna to Shanghai today than it would have been decades ago to plan a trip to Paris or Prague.

Informatizing the *governance* of cities and other communities is the next big opportunity to be seized. Its economic potential promises to be as enormous as the economic potential of governance in general. We are living in an era characterized by the lack of innovation in the creation of new markets into which the economy could expand and consequently the imminent end of economic growth. In such *postgrowth society*, as sociologists call it, public resources are getting more and more scarce, resulting in violent struggles for their redistribution that lead to the collapse of societies. This is where *governance informatization* can offer an escape path and contribute to the prevention of the decline of our civilization. But that is not its only value. Informatizing governance can be an opportunity of epic scale that advances civilization to entirely new dimensions. What makes *governance informatization* possible is the availability of the cyberspace—a dimension for interaction that humanity simply did not have before our generation. The tools our ancestors had at hand were all either bound to the tangible elements of the real world or confined in the private virtuality of one's own mind and soul (as was the case with stories, myths, and ideas). The quasi-tangibility of cyberspace is truly something radically new.

The modern culture of governance is one that is bureaucratic in nature and one that relies on elaborate systems of credentials, on bureaucratic assertions, on rubber stamps and societal roles, on offices, on agents, on administrative mistakes and corruption, on courts and prosecutors, and on systems of checks and balances, among many others. It is a culture that gives work to a chaotically growing public apparatus. The culture of modern bureaucracies is one that evolved centuries ago and has perpetuated itself into the digital age. This ancient culture has evolved from opportunities of the past, which were seized by clans and networks in order to ensconce themselves in the hierarchies of societal power. Political parties, national banks, or health-care systems are examples of such past opportunities that have been grasped and (over many generations) cultivated into the firm societal institutions of the present. However, the digital age offers new opportunities that allow new networks and clans to reimagine and reinvent public governance, as if for the first time.

An example can be found in the governance of credit transfers. Primitive barter of goods and services, as the most basic form of trade, has given way to systems of credit based on coinage, giving way to checks and certificates and finally resulting in fully informatized credit transfer introduced in the 20th century in the form of, for example, the SWIFT system for interbank credit exchange. Each advancement in the evolution of credit transfer was possible for two reasons: One, new technology made the advance possible from a technical perspective, and two, the thus possible advance was a lucrative economic opportunity to be seized. The opportunity for individuals and organizations to become rich by modernizing credit transfer has led us, in less than a century, from minted coins to fully informatized electronic statements that make up currency as we know it today.

Tangible tokens to convey value and assertions are becoming a matter of the past. The evolution from gold to informatized statements to transfer credit is just one such example. Another such example is the evolution of the stock market, which evolved from the paper-based certificates that were used during the first decades of the 20th century to informatized stocks that can be traded by advanced means involving artificial intelligence and computer algorithms—high-frequency trading cannot even be imagined without informatization.

Technical superiority is a proved enabler for taking over entrenched cultures of governance, systems of power, and economies. The naval superiority of the Europeans due to the invention of the carrack led to the decline of the once mighty Silk Road routes, on top of which the oldest known civilizations evolved. The logistic and tactical superiority of the Mongols led to a rapid expansion of the Mongol Empire from the Sea of Japan in the east to close to the Adriatic Sea in the west. The industrial superiority of the North Atlantic powers gave rise to the modern Western civilization, which endures due to technological and military monopolies and the networks of a self-perpetuating public apparatus.

The vulnerabilities of the unchallenged culture of the modern public apparatus show themselves in increasing public debt, increasing taxation, reduction of personal freedom, and a continuing loss of legitimacy of democratic institutions, such as politics, in the eyes of generations raised into the postgrowth society. The rubber stamps and certificates that once were celebrated symbols of progress and prosperity are turning into mere relics of systems that overstayed their welcome. Nonetheless, this rift between the generations is the opportunity for new cultures to emerge—the dusk of the old is at the same time the dawn of the new.

Informatizing governance is about discovering and realizing the technological potentials of the digital age to reach ultimate sophistication in governance. It is an opportunity for the builders of technology to emancipate themselves from the role of mere providers of architecture and for new structures of power to emerge, as well as for existing systems of societal organization and administration to undergo an unprecedented revival and rejuvenation. It is about the renaissance of civilization, a reincarnation of prosperity, the rise of new possibilities and ecosystems, and the utilization of the new-found lands within cyberspace.

This book is about the search for technology to enable governance informatization and about discovering the economic opportunities that come with it. Governance informatization would result in a future in which the organizations and individuals that govern society derive their legitimacy from informatized eligibilities stored in a *timeless* technological infrastructure. This infrastructure would not constrain the scope and mission of such organizations, but would allow the sovereign body of power to interact through a technical platform in order to steer (empower, disempower, control access to resources, etc.) the individuals and organizations. This core infrastructure would contain all data on explicit relations within the society and act as a focal point around which new technical, digital, and social ecosystems would evolve. As such, *informatizing governance* is more than a mere fashion statement. It is not about introducing sensors, reengineering administrative procedures, or replacing rubber stamps for electronic signatures. Rather, it is about a fundamental change of paradigm that is an opportunity of the 21st century for new circles of power to emerge and to build and cultivate their dominions.

This book is structured into four distinct parts, each of which aims to address a specific area of knowledge required to understand the issue in its entirety and, more specifically, to understand where and how to grasp the economic opportunity that lies within.

Part I explores the role of governance in society, the role of the bureaucratic class, and the withering away of the state into an all-encompassing public apparatus (Chapter 1). This is followed by a critique of digitalized governance (Chapter 2) and digital democracy (Chapter 3). Finally, Chapter 4 discusses why written law fails to adequately govern actions in cyberspace. This part thus aims to provide the background knowledge required to understand the context in which this book is placed.

Part II aims to provide the reader the conceptual toolset required to understand how systems of governance come to be and how governance is exercised. To achieve this, the evolutionary principles of systems of power from the primitive emergence of power to elaborate civilizations shall be explored—based on thought experiments in Chapter 5. This shall be followed by a summary of relevant jural theories that aim to provide the structure required to discover and understand the elemental principles that make up systems of law (Chapter 6).

Part III is focused on utilizing the knowledge gained in Part II in order to identify and explore the opportunities of new technology. To this end, an analysis of how technology can be utilized to control governance is explored (Chapter 7). Chapter 8 critically discusses ideas for controlling governance by means of technology that seem relevant at first glance. The search on how to provide informatized governance shall be continued in Chapters 9 and 10 through the development of models and a conceptual framework for technology-enabled governance informatization. Finally, Chapter 11 discusses the vast economic opportunities that lie along the path toward informatized governance.

Part IV discusses how the blueprint developed throughout Part III could be brought to life using existing and well-established technology (Chapter 12) and how legislation would look in a society that adheres to noninterpreted governance. To this end, a system of directly machine-executable legislation is discussed (Chapter 13) and validated against common present-day scenarios (Chapter 14).

PART I

How Technology Challenges the Bureaucracy?

The guiding issue of the first part of this treatise is the tension in the relation between providers of social functions (such as infrastructure, law and order, and public health care) and the citizens, who are addressed by these bureaus and who ultimately pay the bill for the existence of these bureaus. The relation between these two parties is a complex one. Bureaus, in the best case, play a symbiotic role with the citizens, though this can easily turn into a parasitic situation, resulting in *failed states*, societal instabilities, and the wrecking of civilizations. To administer and steer this relation, systems and mechanisms of control have emerged as special social functions, which enabled stakeholders to steer bureaus or pull the breaks, if necessary. Systems like this are then the legislative systems (parliaments, city councils, etc.) of this world, systems of checks and balances, systems of administrative law, and so on.

However, with the introduction of information technology, the rules of the game of social-service provision have suddenly become significantly more complex. What was once about tangible things like people (and their ideas or knowledge), money, and physical borders has become a matter of virtualized entities, long lines of computer code, and complex technical domain knowledge for which traditional legislative, administrative, and legal systems have not been designed. Aside from this, the culture of human interaction has shifted from a prevailing face-to-face interaction in the pre-digital age to machine-mediated exchange (e-mail and social media) or self-service interaction, which no longer requires any human partner. The result is a clash of paradigms in which traditional bureaus lose their synergetic role due to a fading ability to keep up with the times, while their clumsy efforts to modernize further relegate them to the parasitic role of progress-stifling self-preservation.

The emergence of new, tech-savvy bureaus that understand and embrace technology opens up an entirely new set of issues. While on the one hand utilizing the power of digital-age technology to develop new social functions is straightforward and intuitive, on the other hand, there are, as of today, no tools yet to control it. This in turn means that tech-savvy bureaus obtain technology that makes them so powerful that they slip out of societal control. Such bureaus become monopolists, who sit at the longer end of the lever when it comes to balancing the power relations in a society. Once a tech-savvy bureau reaches a de facto monopoly status, society becomes locked in an immutable relation toward such a bureau, and the bureau becomes an absolute ruler over their particular realm that can barely be challenged. The threat of such bureau lock-ins has risen to an unprecedented level with the technological complexities brought about by the digital age.

The overall conclusion of this part is that in order for governance to make a leap into cyberspace, new systems of control need to be found and designed, to adequately address the changing circumstances brought about by the digital age. Awareness of the outdated nature of established systems for controlling governance, such as written law, is essential. These mechanisms are incapable of assuring democratic control of the technological systems that provide governance. As society has no adequate means to democratically control these technical systems of governance, we run the risk of drifting into a neo-feudal order dominated by überpowerful bureaus.

This part is organized as follows: Chapter 1 aims to explore the culture of bureaus and their intrinsic inclination for self-preservation and expansion. This shall aid in understanding the threat posed by überpowerful bureaus and the consequent need for adequate mechanisms of control. Chapters 2 and 3 discuss modern research and development activities aimed at technicizing governance and the modernization of bureaus by means of information and communication technologies. The objective of this discussion is to illustrate that the trajectory on which the evolution of these technologies stands is one that fosters the emergence of technological monopolies, rather than preventing them, and hence is one that undermines the sustainability of the democratic principles. Finally, Chapter 4 confronts the established system of written law with the core principles of the world of technology to demonstrate that written law is not an adequate system that could govern technological systems for governance.

This page intentionally left blank

CHAPTER 1

Understanding the Public Apparatus: Opportunity, Dominion, Threat

Contents

The world of technology tends to be clear and universal about its concepts—if one wants to buy new tires for their car, they will be able to do so in any part of the world without lengthy discussion with the mechanic on what exactly they mean by using the word "tire." Unfortunately, the same cannot be said for the words we use in the domain in which this treatise is set. When dealing with governance for the common good, one has to deal with concepts such as "bureaucracy," "the state," "democracy," and so on, each of which is everything other than perfectly clear. So, in order to be able to understand, discuss, and criticize the ideas outlined in this treatise, it is paramount to first establish a shared context in which these ideas can be assessed. This chapter, then, is about setting the broad context.

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00001-7

Section 1.1 covers the semantics and the lessons learned from history when dealing with things like "the bureaucracy," "the state," "the government," or "the public administration." As shall be discussed, the term "bureaucracy" has a complex and vivid history, which makes it hard to be used in the modern world, simply for the reason that what our ancestors referred to when using "(the) bureaucracy" has no clear successor in the 21st century. Instead, the concept of the *public apparatus* shall be introduced in order to be used throughout this treatise.

Having cleared up the terminology at stake, Section 1.2 explores the phenomena of the ubiquitous *continuity* of the public apparatus, and its continuous expansion, following the question of why it is logically unthinkable that the public apparatus would ever voluntarily contract. The legacy from modern intellectuals like Cyril Northcote Parkinson (*Parkinson's law*) or Anthony Downs (*public choice theory*) help in understanding the underlying drive that keeps the public apparatus in perpetual expansion.

Section 1.3 aims to illuminate the dark side of the public apparatus, where institutional corruption is part of the game, where the human agents are no knights in shining armor, but rather plain dilettantes, and where the agents and actors of the public apparatus simply follow their own personal interests. To help in understanding the implications of corrupt and immoral behavior of the public apparatus, three real-life cases of administrative incompetence, predatoriness, and sluggishness are presented.

To this extent the bureaucracy and the public apparatus will be portrayed hereinafter from a critical perspective—as systems empowering a self-perpetuating class of agents, which drain economic and societal power away from capital owners like peasant elites, artisans, industrialists, or merchants. Understanding this age-old struggle between those who create and cultivate wealth and those who specialize in redistributing it is important in order to unveil the hidden potentials. To this end, the purpose of this chapter is to raise awareness of the flaws in traditional approaches, in order to expose the opportunities these flaws bear for innovation and renewal. Understanding these flaws will help in understanding how technology can be applied without repeating the same mistakes over and over again.

1.1 TRANSITION FROM THE BUREAUCRACY TO THE PUBLIC APPARATUS

Ancient mythology is rich with fantasy creatures reflecting the many aspects of the bureaucracy or (administrative) systems of power: Minotaur's labyrinth as a metaphor for ancient Greece's administration (Wysling, 2015);

the Hydra, a monster with many heads, where for every head chopped off the Hydra regrew many new heads (Ogden, 2013), as a metaphor for the regeneration feature of the bureaucracy.[1] Kafka's *der Prozess*, a novel about a man who is being arrested and prosecuted by a remote, inaccessible authority, in which the nature of his crime is revealed neither to him nor to the reader, is an allegoric version of the never-ending entanglement with state authorities one experiences when trapped in dealings with the state.

Nevertheless, if one were to ask some random consumer on a Western high street about their opinion on the necessity of the myriad of governmental agencies as a whole, chances are near absolute that the response would be affirmative. The existence, constitution, and symbiosis of the public apparatus in general is not questioned, but rather passively approved with the blind conviction of a religious believer in the righteousness of their respective faith. To such respondents, a world without public schools, social care systems, state army, parliament, courts, police, and taxes, etc., would be plain absurd. Asked for an opinion about the bureaucracy, the same respondent would likely engage in elaborate ranting against lengthy and confusing administrative proceedings, corruption, the lack of justice, and the masses of public officials who (unlike themselves) do not do any actual meaningful work.

We have all encountered similar situations which reflect the duality of the public apparatus: the dogmatic goodness of the systems that govern us on the one hand is contrasted with the incompetence and brutishness of petty bureaucrats and government alike. Just as Brecht's (2003) fishes have been groomed by the sharks to swim right into their throats, the modern public have been groomed to subject themselves to the status quo of the public apparatus—it has become the water in which we swim.

1.1.1 What is the Bureaucracy?

The modern understanding of the concept of *bureaucracy* is fuzzy, but polarizing nevertheless. It is fuzzy because it has a variety of different meanings in the public, in scholarly discourse, among a whole spectrum of other uses. It is polarizing because the associations it provokes are deeply rooted in personal experience and worldview. A typical association that emerges when hearing the word "bureaucracy" is the delivery of social functions—i.e., the provision of services that serve the community at large (e.g., the police force, public health-care systems, and the legal system).

[1] Albrow (1972, p. 20) refers to an 1836 essay on the French education system, which points out that each fault in the bureaucratic apparatus was cured by establishing a new bureaucratic apparatus. For an inherent motivation of bureaus to reproduce, see also Downs' *Inside Bureaucracy*.

In this capacity, bureaucracy is sporadically bashed by reformist movements, which would rather see private companies delivering certain social functions (private schools, private hospitals, private buses, …), while conservatives don't hesitate to respond by emphasizing the bureaucracy's role in defending stability (Bannister, 2017; Olsen, 2006). Such scholarly pro- and contra-discussions on how to reorganize (if at all) the delivery of social functions are deeply entrenched in ideology, though they remain rooted in the same culture they support. In the context of such debates, the term *bureaucracy* is understood as Max Weber's model of hierarchically organized public administration. This model is based on a rational-legal order, in which professional administrative staff deliver (or administer the delivery of) social functions. However, Weber is often erroneously attributed to having defined bureaucracy, while, in fact, he himself never actually provided a definition of this term (Albrow, 1972). The modern notion of *bureaucracy*, as used by the proponents or challengers of Weber's ideal type of organization, is one that has grown with time. However, this evolution of terminology departs from the original semantics of the word itself.

In tracing the origins of this term, one such occurrence was found by Albrow (1972) in some letters exchanged between Baron von Grimm and the French Administrator of Commerce, de Gournay, in 1764–65. In these letters Baron von Grimm complained about the proliferating *bureaucracy* of offices, clerks, inspectors, and intendants, who were not appointed in the public interest, but rather, the public interest having been established such that the bureaucracy could exist. In this context, *bureaucracy* stands for a form of societal rule, a form different from aristocracy (from Greek *aristos* = excellent—"rule of the best"), monarchy (rule of one), or democracy (*demos* = commoners); thus, bureaucracy stands for "rule of the bureaus."

Since the 18th century different branches of research and debate have emerged around the term *bureaucracy.*[2] However, the narrative of the *rule of the bureaus*, whose prime aim is self-preservation, remains a dominant

[2] Albrow (1972: *Bureaucracy*) distinguishes three notions in 19th century literature: first, being a separate form of rule next to aristocracy, monarchy, or democracy; then a German view focused on the organizational form of the German public administration; and finally a citizen-centric critique on state performance, similar to modern criticism of "red tape." Also Downs (1967: *Inside Bureaucracy*, p. 26), though not aware of Albrow, distinguishes three notions, namely bureaucracy as an ecosystem of bureaus (which constitutes a societal class of its own), a method of allocating resources within large organizations, or "bureau-ness"—a quality that distinguishes bureaus from other types of organizations. The latter two of Downs' notions come close to Weber's model of organization; however, Downs fully advocates the first notion (i.e., the self-preserving ecosystem, or class) as a crucial principle of operation.

one throughout the 20th and 21st centuries. In this narrative, a bureau does not exist to satisfy public interest, but rather public interest is advocated to provide means for the existence of a bureau. As a consequence, the continuation of these bureaus is justified for no better reason than to provide work or other "added value" results for its employees and stakeholders, both internal and external. The understanding of *bureaucratic* as denoting the growth of bureaus without any substantial need has been adopted also by the *Académie Française* as one of the two semantics, the other being the influence of government agencies (Albrow, 1972, p. 15).

1.1.2 The Bureaucracy: A Job Creation Scheme

The opinion that bureaus' missions are an end to themselves is surprisingly natural and widespread both in space and time, as well as being culture-neutral. It is not a distinct school of thought, such as Weber's concept of bureaucratic organization and authority, but instead occurs by virtue of knowledge gained as individuals from personal (often professional) experience from involved interaction with bureaus. Such is the experience of Prussian official and statesman *Heinrich Friedrich Karl vom und zum Stein*, who in an 1821 letter criticized the self-perpetuation of a penniless class of civil servants (Albrow, 1972, p. 17). Another such example is *Cyril Northcote Parkinson*, a former member of the British military during the decline of the British Empire, who coined what is known today as Parkinson's law (Parkinson, 1955): work expands so as to fill the time (or resources) available for its completion. Similarly, *Alfred Walter*'s (a former civil servant) impression of the contemporary German bureaus (Walter, 2011) is one of a world in which everyone works as much as they want and as well as they can. Likewise, the previously mentioned *Jean Claude Marie Vincent de Gournay* and *Friedrich Melchior Baron von Grimm* were high-ranked and experienced civil servants in 18th century prerevolution France, witnessing the dawn of modern bureaucratic culture; furthermore *Milovan Đilas*' (Djilas, 1957) view on the communist system as the struggle of an emerging bureaucratic class to take over rule is grounded in his firsthand observations throughout all the ranks of the Yugoslavian communists.

Valuable firsthand accounts of bureaucracies' intrinsic nature of self-preservation, and expansion of dominion, come surprisingly often from those who have reached the peaks of revolutionary, postrevolutionary, or precollapse bureaucratic hierarchies, and thus have gained as much as they could gain before switching sides, after retiring, or after experiencing the transition to a new order. For example, Đilas documented his insights into real socialism while serving prison time in postrevolution Yugoslavia.

If we adopt the view that *the bureaucracy* is an ever-growing organism of bureaus, many of which exist for no impartially comprehensible reason, we can see an underlying characteristic of the bureaucracy: it is a giant job creation scheme born and propagated out of opportunity, rather than necessity. The bureaucracy has long outgrown the narrow scope of a formal system of power, or its public administration. Instead, its sphere of influence has been extended to form a *public apparatus* together with actors from domains such as the military, police, intelligence services, education, academia, politics, legislation, media, construction, health and social care, public finance, law enforcement and judicial sector, international organizations, and nongovernmental organizations (NGOs).

The term *public apparatus*, as shall be used throughout this treatise, refers to a complex fabric of agents who existentially rely on public resources (taxes, natural resources), which they control, govern, and distribute. The methods of operation of the public apparatus include various forms of state intervention, subventions, and other ways of entanglement with otherwise private-domain affairs and activities.

Among early works that criticize the creeping expansion of the bureaucracy is John Stuart Mill's *On Liberty* (1859). Mill writes disapprovingly of the way the government has endlessly extended its repertoire of provided social functions, thus providing ever new career possibilities within the bureaucracy itself, which, in turn, attract new leeches to feed off the possibilities provided by the *public apparatus* (Albrow, 1972, p. 21).

The emergence and growth of the modern Western public apparatus correlates with the 18th century urbanization that occurred in the transition from agrarian to industrial society. Accordingly, it also correlates with the emergence of a public sphere (Habermas and Burger, 2008)—a sphere for public discourse which is dominated by media and politics, two powerful branches of the public apparatus. The modern public apparatus relies vitally on the massiveness and density of cities and their public spheres—a product of the industrial society. The modern public apparatus has grown into a structure that governs nearly all aspects of modern life. Peasant societies, or nomadic tribes, which relied heavily on manual labor for survival, had few means to develop complex systems for administration or policy-making. On the other hand, urban society and industrial society, even more so, present an excellent breeding ground for the development of public interest: labor unions, public hygiene and health care, social insurance schemes, public schools, publicly funded research, labor market governance, workers' rights, urban planning, municipal infrastructure, etc., can all emerge as matters of public interest to be taken care of by the public apparatus.

With the increasing complexity and expansion of the public apparatus, the boundaries between the bureaucracy as a separate class, and those who are governed by the bureaucracy, gradually wither away. While the patriarchal peasant elite in 16th century Germany were more powerful in dictating terms against the aristocracy when negotiating the conditions of their mutual coexistence (Robisheaux, 2002, chap. 5), the modern German farmer must rely on farm subsidies, thus being made part of the public apparatus, and is subjected to the public interest as such. The single-party systems of the Fascists, Nazis, early Communists, and many post-WWII political parties used party membership to distinguish members of the ruling class from nonmembers (party membership was required to attain influential positions in the state, academia, etc.). This distinction provided a certain clarity of the class separation (Djilas, 1957); however, this distinction has since vanished. Thus, while it was comparatively easy to define the boundaries of the communist nomenklatura, it is near impossible to identify the de facto key stakeholders in modern informal networks of power that govern the public apparatus.

1.1.3 Patterns of Bureaucratization

If we observe the recent struggles for power of communist networks during the revolutionary/postrevolutionary period, we gain insight into how a bureaucracy (in terms of class) emerges by seizing the available opportunities. The communists' way of seizing opportunity was simply theft: through ideologically justified expropriations of capital owners, the penniless supporters of an emerging new bureaucracy transferred (nationalized/collectivized) private capital into the dominion of the public apparatus, where it served to equip the new elites.

Within the last century, such methods were exhaustively applied in the socialist Warsaw Pact states, Yugoslavia, China, Albania, and Peru, among others. In postrevolution (i.e., post-WWII) Yugoslavia, wealth was systematically nationalized in the form of agrarian land, real estate, factories, company shares, commercial stock, etc. This was done through law, murder, or dubious court trials. Consequently, this gained capital fueled the public apparatus of the new systems, and continues to do so in the 21st century. In Slovenia, a successor of former Yugoslavia, the bureaucracy occupies itself with posttransitional implications like restitution (Paulin, 2009), privatizations of national property, and the corruption that follows (Frangež, 2007).

In Peru, the 1986 coup d'état by the armed forces led by Juan Velasco Alvarado aimed for a similar approach. Alvarado's regime aggressively enforced existing land reform provisions and expropriated the estates of wealthy farmers, giving land to propertyless agricultural workers and tenant laborers—the *campesinos*—who formed a quarter of Peru's population back in 1961 (Ballantyne et al., 2000). Alvarado's regime raised a system that offered the campesinos services such as credit through the state bank, or subsidized fertilizers (Ballantyne et al., 2000). However, the sustainability of Alvarado's system was short, and within two decades corruption in the course of decollectivization overshadowed the ideological goals of the reforms (Ballantyne et al., 2000).

Communist rule in Albania left property relations in a mess: In 1950, more than 90% of the land was owned by private owners; in 1989, only 3% was not part of the public apparatus; and again by 1995, almost 95% was once more in private hands (Cungu and Swinnen, 1997, in: Ballantyne et al., 2000, fig. 2). Though such fluctuation is not unusual in former communist countries in which postwar nationalizations are rolled back by posttransition restitution laws, in part Albanian society adheres to the ancient customary canon law, in which property is clan-based, rather than bound to a specific person (Trnavci, 2008). Unlike in Former-Yugoslavian Slovenia, where posttransition restitution aimed to repeal the post-WWII land nationalizations, Albanian decollectivization was conducted through nine different privatization programs, where land was partly allocated by lottery to peasants (Ballantyne et al., 2000). The attempt to enforce Western-style land ownership in postcommunist Albania resulted in riots, corruption, system breakdown, and anarchy (Lemel, 1998).

Establishing a public apparatus based on expropriated capital is a *shock-and-awe approach* to creating a new realm for a bureaucracy to grow in. The first steps of a budding bureaucracy are humble, and for the pioneering generation it is easy to build a career (Bajt, 1999), thus setting the foundations for a new era. This approach is then the first pattern of the beginning of a new bureaucracy: the capital of the defeated class becomes prey to the new class (Djilas, 1957). This *shock-and-awe approach* is the first pattern of bureaucratization.

A second pattern is the *creeping bureaucratization*, in which an existing bureaucracy slowly expands by inventing new social functions via an existing relation with capital owners. This form of gradual bureaucratization can be observed in the relation of Austria's monarchy and its rural society during the first half of the 17th century. Hermann Rebel's *Peasant Classes* (Rebel, 1983) focuses on the process of slow transformation of the Austrian state bureaucracy into an all-encompassing public apparatus, with welfare state implications. His focus of study is the Upper Austrian Crown lands, but the same principle may be applied to other areas of the realm.

> *Even before the outbreak of the great peasant war of 1525, then, the Austrian peasantry's status, economic welfare, and social structure began to appear as a significant element in the formation of the absolute state. For the following three hundred years, the rural population became the football with which princes and nobility played the games of state-building and status-maintenance.*
>
> ***(Rebel, 1983, p. 4)***

The traditional patriarchal society of the rural population was organized in hereditary estates (manors/"houses") to which the rural population was subject to. The hereditary rules maintained a male success to the manor, with the other sons finding refuge among the clergy or in cities.

The serfs of the manor belonged to the estate, or lived freely as a "masterless" class, living in small cottages and working as woodworkers, charcoal burners, basket makers, or similar, or joined the cities. The growing population of the masterless and the troubles associated with them were an appealing territory for the bureaucracy to expand into:

> *State-managed factories such as the woolen mills in Linz or the workhouses of Vienna were in effect substitute house administrations for the unemployed and unattached. Beginning in the 1680s, masterless children were "legitimized," i.e., attached to peasant house communities by state and estate authorities where they could be supervised and put to work. [. . .] This Austrian welfare state, which worked by enlisting families, households, and publicly managed houses into its poor relief administration, survived well into the nineteenth and, in some of its aspects, the twentieth century.*
>
> ***(Rebel, 1983, pp. 144–45)***

The growth of the masterless population, and the recognition of its welfare as a mutually agreeable matter of public concern, was the gateway for a creeping bureaucratization toward workhouses, orphanages, public schooling, public health, pension schemes, and a further prolific expansion of the public apparatus.

A third pattern is the *homecoming* of a bureaucracy in the course of the contraction of an empire, or the contraction of wealth on which a bureaucracy relies. The last observable contraction of a bureaucracy's dominion was the British Empire's rapid decline after WWII. To the British, their Empire provided a realm to export the surplus of population for centuries, a refuge for penniless adventurers, and a source of wealth on which the British bureaucratic class could feast outside the homeland. While continental Europeans struggled with the rise of domestic bureaucracies throughout the 17th–19th centuries, British intellectuals considered themselves exempt from this supposedly continental phenomenon (Albrow, 1972, chap. 1). However, the rapid contraction of the Empire yielded a surplus of veteran bureaucrats from overseas who found a new home in the expanding British domestic public apparatus (Parkinson, 1955).

While the British homecoming was physical due to the contraction of a physical (global) realm, countries like Saudi Arabia experienced contracting realms of their bureaucracies in terms of a sharply declining oil price. With lavish bureaucracies accustomed to relying on wealth acquired by the dominion over the black gold, they turned to domestic tax residents to support the continuity of the public apparatus by severely increasing taxes, cutting subsidies, and fortifying their tax exaction apparatuses.

1.1.4 Going Global: Who Pays the Bill?

Manuel Castells called the sum of the changed circumstances caused by globalization the *network society* (Castells, 2010). However, as work, society, and economy became global, agile and flexible, so did the spheres of interest and influence of bureaus become global, agile, and flexible, by incorporating informal networks and ad hoc relations in overcoming former narrowness and rigidity of the bureaucracy. The intertwinedness of the bureaucracy with the general population challenges the concept of a separate ruling class, and against the backdrop of the network society, concepts such as the state wither away, while the public apparatus becomes global (Graeber, 2015).[3]

A community's public apparatus is perhaps best understood as a system of organizations, and their programs and activities, which are ultimately funded by the community—either actively upfront or passively through suffering of the consequences. For example, the US tax residents finance (without consent and often against their will) the global activities of the bureaus which spread terror and chaos in foreign places. Much like the subjects of the Third Reich financed the hostile expeditions of their empire, only to pay the bill a second time when foreign bombs destroyed German

[3]Graeber acknowledges that *bureaucracy* is not a fitting description in the 21st century (Western nations) any more, since the boundaries between system and society have dissolved. For lack of an existing term, he christens the new concept *total bureaucracy*, but rarely uses this term himself. Unfortunately, he uses all three main semantic notions of *bureaucracy* concurrently—namely bureaucracy as a separate class, bureaucracy as a system of organization, and bureaucracy as the system of communication by means of forms. As such, his *total bureaucracy* refers to the reflection of the explosion of the relations caused by/linked to the myriads of public apparatus actors, which is going on approximately since the decoupling of the US dollar to gold in 1971 (Graeber, 2015).

property, a third time after the loss of the war by suffering reparation payments and destroyed industry, and a fourth time with an ever-increasing national debt. The costly adventures, escapades, and sins of the public apparatus have always been a cause of concern and conflict in relation with tax payers. On the other hand, it can become a point of contention between rivaling branches of the public apparatus. In essence, it is a fight over resources, which capital owners surrender to avoid harm, and the public apparatus soaks up to satisfy their own needs.

Modern nation states, as the classical model (Jellinek, 1905) suggests, consist of the state territory, constitutive people, and state power. This model is a reasonable tool for philosophy and diplomacy in the post-Westphalian[4] order, in which the sphere of influence and action of nation states is confined to a national territory. However, the *imagined community* (Anderson, 2006) of the nation state, and hence the ability and duty to influence the course of a nation state, gave way to incoming international and supranational structures of power, to reach the point now where the concept of nationality itself is ripe to be challenged. The formal definition of a nation state, however, is of no relevance in the question of who is paying the bill—it does not matter if the extent of a community's public apparatus remains confined to a national territory or if it stretches out globally. One way or another, it is the "home" community of a public apparatus which is called to fund the programs of its bureaus in form of taxes, slavery or low-paid labor, environmental destruction, corruption, expropriation, injustice, domestic conflict, and violence. Correspondingly, it is this "home" community to which the public apparatus offers new employment opportunities and new opportunities for economic outreach and prosperity.

1.2 IMMORTALITY OF THE PUBLIC APPARATUS

> *They have survived the changes from monarchy to republic, from republic to dictatorship, from dictatorship to democracy; in times of political collapse they had to bear the burden of public action. The bureaucracy is older than the democracy.*
>
> ***(König in: Walter, 2011, own translation)***

Established ruling networks often maintained and improved their privileges within and beyond the existence of states. In spite of the challenges that

[4]The peace treaty of Westphalia was the formal act ending the Thirty Years' War—a series of armed conflicts that raged in 17th century Europe, ringing in the twilight of feudalism and the dawn of the bureaucracies.

changed circumstances (new kings, governments, ideologies, political systems, etc.) entail, established networks of power tend to adapt in order to maintain the continuity of their privileges, and keep "one foot in the door."

1.2.1 The Continuity of Networks

When East European states rid themselves of the socialist constitutions in recent history, hopes were high that Eastern Europe would soon catch up to Western Europe in terms of development. What followed, however, was wild privatizations of former state property, the rise of an extravagant *nouveau-riche*, and expanding crime and corruption. More than 20 years after the formal fall of East European socialist orders, it became clear that the social networks in power before the fall had survived the transitive period and managed to secure many of their own privileges.

The modern Russian Federation's elected leader Vladimir Putin was no outsider to the Soviet nomenklatura, but rather an active member. The "fall" of the Soviet Union was, obviously, not the fall of the networks of power that fed the political entity, but rather it was a structural transformation from one fashion of reign into another. This differed from past revolutions, such as the worldwide communist revolutions throughout the first half of the 20th century, or in the Islamic revolution in Iran. In these revolutions, a new class rose to power through bloodshed, expropriations, and expatriations, though the European ex-communist networks merely changed facades while maintaining communist symbols, traditions, and formal structures of youth recruitment.

Dzero (2011) writes how this looks in modern Russia:

> *The body of the revolutionary Vladimir Lenin continues to lie in the mausoleum and the Soviet Red Stars still adorn the Spasskaya Tower of the Kremlin. The Soviet era continues to be represented on metro stations and street names—Oktiabr'skaya' (named after the October Revolution), Biblioteka Lenina (Lenin's Library) and even Marksistskaya (Marx'). […] With at least half of mainstream TV sponsored or owned by the state and promoting the glorification of Soviet events such as the Great Patriotic War, it is no surprise that many (especially Western critics) seem both critical and confused as to the intentions of the Kremlin.*

A similar picture is drawn in EU, NATO, and OSCE member state Slovenia, where state politics and administration have been (since the state's separation from Yugoslavia in the 1990s) dominated by the social networks rooted in socialist-era bureaucracy. Balut and Cabada (2000) describe the dissemblance of the Slovenian Communist Party into a multitude of smaller parties. These parties later partly reassembled and continued to control the

Slovenian state through the public apparatus—i.e., through politics, media, state agencies, public administration, unions, NGOs, and ownerships in public and privatized corporations.

Players in these social networks in many cases "were cynical careerists who joined the parties, not because they believed in them or their ideology, but because they believed in the durability of that system and knew that their ambitions could only be quenched within it" (Boduszynski, 2000)—in short, they seized the opportunity to join the "free-for-all" *public apparatus*.

1.2.2 The Continuity of Culture

The (German) *culture*[5] of the bureaucracy began to develop in the mid-17th century, when strong principalities managed to monopolize their power over entire countries, thus superseding the previous decentralized feudal structures (Mayntz in: Walter, 2011, p. 23). In order to maintain their power, these rulers required stable power bases which were independent of the voluntary contributions of feudal fealty. This basis was found in standing armed forces which were financed through novel systems of taxation. In order to administrate both taxation and military, public administrations were born, endowed with the required powers (Walter, 2011, p. 24).

In the beginning of the 19th century, fundamental reforms in the administrative and justice systems took place under the influence of Napoleon's conquests in Prussia and the states of the Confederation of the Rhine. In this course, the judiciary had been separated from the administration, while a system of local self-government was introduced to cities and municipalities. Further, specialized agencies responsible for ordnance survey, land consolidation, road construction, telecommunications (mail and telegraphy), railways, etc., were established. The administrative system was split into three layers: upper-layer authorities (ministries), middle-layer authorities (district governments of various kinds), and other further lower-layer administrative units. This allowed the separation of territorial and functional concerns to a certain degree. The upper-layer government had the possibility to work through separate ministries. At first, these were the ministry of foreign affairs, of war, of finance, of justice,

[5]The *Oxford English Dictionary* defines *culture* as used in this context as the "distinctive ideas, customs, social behavior, products, or way of life of a particular nation, society, people, or period. Hence: a society or group characterized by such customs, etc.," or "a way of life or social environment characterized by or associated with the specified quality or thing; a group of people subscribing or belonging to this," or "philosophy, practices, and attitudes of an institution, business, or other organization."

and of the interior. The lower-layer administrative units were responsible for enforcing government policies and represented the state toward common citizens by supervising affairs in the municipality, providing police, issuing passports, taking care of recruitment, collecting taxes, building roads, etc. (Walter, 2011, pp. 25–26).

Throughout the first half of the 19th century, the public administration grew substantially into a vast machine. This rapid growth contributed to the tensions, which ultimately culminated in the European revolutions of 1848–49. After the German 1849 March Revolution, the Frankfurt Assembly, which was working on a (later rejected) constitution for a German state, did not dare to alter the structures of the already robust bureaucracy, nor were they changed by the *Reichsgründung*—the foundation of the German Reich in 1871. The German public administration was further extended and enlarged through to the end of the 19th century. The number of ministries grew, as did the number of specialized departments, inspectorates, etc., and novel social and community functions were introduced (Walter, 2011, p. 26).

The continuity of the German state bureaucracy (in terms of the public administration) has already been emphasized by Weber (Walter, 2011, n. 2), who noted that the administrative machine "simply continues to serve the violent revolution and the occupying enemy as it did for the so-far legitimate government." Thus, the German public administration system survived the end of the constitutional monarchy in 1918, the takeover by the Nazis in 1933, and their fall in 1945 (Walter, 2011, p. 27).

The toleration and cooperation with a preexisting bureaucracy has been valued by Fascists (Albrow, 1972, p. 93) of the post-WWI era and Persian warlords after the fall of the Safavid Dynasty (Amanat, 2011) alike, while the Bolsheviks (Albrow, 1972, p. 85), Napoleon (Kranjc, 2015), and the Iranian Ayatollahs (Kurzman, 1996) went for a blank slate approach, purging the old structures of continuity. The system of power pursued by the Bolsheviks (in Lenin's theory) was about the elimination of the bureaucratic (bourgeois) class in favor of a classless society in which *everybody* would be a bit of a "bureaucrat" (Albrow, 1972, p. 87). The Ayatollahs strived for a decentralized Sharia-based system that was incompatible with the structure of the preceding monarchy. Napoleon introduced his own form of administration, instead of attempting to rule over a fragmented and highly complex feudal system in the conquered realms. In these cases, a fresh start, which partly incorporated the local national peasant elites, was practical.

The capacity for culture (in terms of practices, customs, and worldviews of a particular nation, society, people, or period) to perpetuate itself for no better reason than the common understanding that things in a certain sphere *have always been done that way*[6] makes for a robust stabilizer, when cultivated and maintained in the context of power. It is important to keep this power of culture in mind in the context of the present treatise. On one hand, challenging or eradicating a culture (existing power relations, types of institutions, and ways of conduct) will inevitably imply reactionary resistance, but on the other hand, once a shift to a new culture is successfully conducted, the stabilizing feature of culture will protect and legitimize the transformation.

Existing culture is an ever-present stumbling block for disruptive change, as the case of the recent introduction of a land registration system in Albania in the 1990s demonstrates. This case gives a present-day insight into an ongoing shift of culture from a prebureaucratic patriarchal society to a Western-style system of land registration (Trnavci, 2008). While new networks of power tried to introduce a new culture of governing property rights in the domain of land ownership, the rural clans in Kosovo[7] and north Albania resisted this shift and continue to adhere to their customary canon law that survived Christianization, the Ottoman Empire, and communism. This resistance discouraged (and continues to discourage) the further influence of institutions of the bureaucracy and preserved an ancient peer-to-peer legal and social system.[8]

[6]The "Five Monkeys Experiment," though merely a popular Web meme and urban legend, rather than a real experiment, provides a good explanation: In this thought experiment, five monkeys in a cage are collectively penalized when one of them tries to reach for a banana on a ladder, thus learning to avoid the banana. One monkey is replaced for a newcomer, who, when aiming for the banana, is beaten by the group and thus forcibly prevented from the banana. One by one the monkeys are replaced, until none of the monkeys in the cage knows the original reason why everybody beats whoever aims for the banana. Another good picture of the self-perpetuation of culture in the context of rituals can be found under the term *cargo cult*.

[7]On a side note, the violence of ethnic conflicts in Kosovo and FYR Macedonia, which involve Albanians (Shqiptars), has its roots in these very cultural differences between the ancient Shqiptar society and the modern trust in a central state by Serbs or Macedonians, respectively.

[8]Other than that, the culture of their peer-to-peer system is odd from another perspective: members of a prebureaucratic clan might find it strange not to assist materially their family members who do not engage in a gainful occupation—members of a modern womb-to-tomb social state on the other hand might find it strange to do so, given the existence of state institutions that are there to provide material aid.

1.2.3 The Continuity of Bureaus

The motivation and rationale of the organizations of the public apparatus (bureaus) have been explored by the public choice theory (Buchanan et al., 1980; Downs, 1967) and its followers. Public choice is about making rational assumptions of human behavior when set in the context of power or public office. It assumes, in general, that the incumbent individual will adopt a behavior that they expect to be helpful in sustaining or prospering their personal life situation with regard to career perspectives, income situation, or social status.

Anthony Downs' *Inside Bureaucracy* (Downs, 1967) aims to explain the state of a public apparatus as a result of the self-interest of individuals who drive the creation and development of institutions (bureaus) and perpetuate their existence. *Bureaus*, as defined by Downs, are large, professionalized, nonmarket organizations that aim to provide social functions to a given target group. Downs identifies four ways in which bureaus come to life:

(1) as the routinization of charisma, in which followers of a charismatic leader transform themselves into a bureaucratic structure to follow the leader's ideas and vision;
(2) from scratch, to address a need perceived by a specific stakeholder group in society;
(3) as a split-off from an existing bureau; or
(4) through entrepreneurship as the result of agitation of a small group of activists who call for the realization of a specific idea.

Once established, a bureau aims for its perpetuated existence, which requires regular income for sustenance. The nonmarket nature of the bureau requires it to be engaged in a mutually beneficial relation with its external supporters. This relation, however, is not based on a continuous verification of the bureau's external efficiency. According to Downs, as the bureau grows larger, the proportion of activities devoted to delivering its primary social functions diminishes, while the resources required by the bureau continue to rise.

Those who ultimately benefit from the bureau, Downs argues, are wrapped in *rational ignorance*—i.e., they tend not to think too much about their relation with the bureau that provides value to them. Correspondingly, the bureau aims for a state of equilibrium with its supporters so as to prevent any tensions that might make them reconsider the bureau's necessity. In relation to the bureau's home base (e.g., the taxpayers) as the effective financer, bureaus aim for "the exemption from antipathy," i.e., they try to maintain a positive image, a perceived usefulness, and hence, a continuation of their legitimacy. This struggle for exemption from antipathy and the upkeep of a positive image is reflected in everyday news, featuring success stories of law prosecution agencies in their fight against moral wrongdoers, by ministries and political parties boasting about their actions and opinions, and by NGOs' street work, protests, and press conferences.

1.2.4 The Continuity of Work

The public apparatus expands to fill the available resources for as long as possible, and then demands more. This inherent principle is timeless (see Adams' (2001) *For Good and Evil* for examples from history) and exists throughout all levels of societal structure. It exists at the level of the entire public apparatus, at the level of the individual bureau, and at the elemental level of the human agents. Thus, at an elemental level, Parkinson's thought experiments on the principles of the expansion of work (Parkinson, 1955) provide valuable insights.

"Work expands so as to fill the time available for its completion" (Parkinson, 1955) was Parkinson's core hypothesis. In order to prove it, he thinks up an elderly lady with nothing but spare time and a busy man, letting them both dispatch a birthday card. This task, which could keep the former busy for many hours, filling the day in search of a proper motif, a considerate message, and a thematically matching postage stamp, would be dealt with by latter in no more than a couple of minutes to have it out of the way. Thus, Parkinson concludes there is no relationship between the amount of work to be accomplished and the resources assigned to it. Hence, a task that can be accomplished by one person in 1 week could easily be assigned to a team of 10 people with 1 month of time available, and as such, they would find enough work to keep all of them occupied for the entire duration.

Work can only expand up to the limit of the available resources, and hence where such resources are not available, work will be accomplished with higher efficiency. Parkinson applied this law to the public apparatus, as it is a system financed by taxpayers with little to zero actual possibility in controlling (or at least having insight into) its complex workflows. This type of "law" cannot be applied to workspaces such as high-volume sweatshops in Asia, in which all available resources are streamlined to maximize output. A significant advantage for bureaucratic organizations in this regard is that their resources can be expanded—i.e., taxes can be raised, public assets sold, or loans taken up when the amount of subjectively desired (not necessarily required or needed) expense exceeds the available resources.

Parkinson claims that the relation between work and the required size of a bureau depends on two factors. *Factor I* is that officials tend to multiply their subordinates (rather than rivals). *Factor II* is that the officials tend to make work for each other. His reasoning for *Factor I* can be expressed using the following paradigm.

A civil servant—let's name her Ann—who subjectively considers herself overworked, will have three options: (a) to resign, (b) to ask for help from a peer at the same level, or (c) to hire subordinates to assist. To resign, naturally, is no option. A division of work with a peer would mean inviting a rival, who could sooner or later endanger Ann's career ambitions. So, the only feasible option is to hire subordinates. Now, it might be economically feasible to hire one subordinate assistant, a young ambitious aid, who would take care of Ann's worries. But hiring one single assistant would mean that there could soon come a time when the assistant would become a competitor to Ann and be able to replace her. The solution, hence, is to *divide and conquer*. Consequently, Ann employs two junior subordinates—Bob and Carl—and assigns them each work in such a way that they remain in competition with each other and dependent on her. Ann can thus control them by keeping them competing for her own position, which she will vacate sooner or later, as she herself will advance. This way Ann establishes a small loyal network with herself on top of the pyramid. Sooner or later, Carl might consider himself overworked too, and Ann will, to not endanger the balance between Bob and Carl, solve this problem by assigning two subordinates to both Bob and Carl.

Ann's team has thus multiplied, and a task force of seven now does what Ann used to do herself. This, naturally, implies danger that members of the group would end up without work to do. To prevent this, a multiplication of assignments has to take place, so that each of the officials gets a part in the process of handling each incoming document. The response shall be composed by the subordinates and handed over to their superiors for authorization, and finally to Ann to approve it. In this way the whole hierarchy is occupied with itself. Ann, being at the top, could decide to simply approve the reply without even reading it, as she is occupied with far more severe worries related to the management of her team, but it would contradict Ann's nature to allow something to leave her office without meeting her high expectations. Thus, Ann not only reads the reply but also rewrites it entirely, spending as much time with the document as she would have if Carl and Bob had never been born. "And it is late in the evening before [Ann] quits her office and begins her journey [home]. Among the last to leave, [Ann] reflects, with bowed shoulders and a wry smile, that late hours, like grey hairs, are among the penalties of success" (Parkinson, 1955).

Parkinson's law implies that the bureaucracy is more about social networks primarily devoted to securing strictly personal interests, rather than organizations that would strive to excel by creating competitive added value for their clients. Breton (1995, p. 435) argues that Parkinson's law is a result of informal social networks, where superiors (principals) are indebted to subordinates (agents) for informal services accrued. To pay off their debts, superiors promote their subordinates to higher ranks or provide them with some other kind of advantage within this hierarchy. McKee and Wintrobe (1993) support this claim, pointing out that "Parkinson's observations are simply evidence of the existence of implicit contracts within organizations."

On a side note, the principles of Parkinson's finding regarding the expansion of work have been supported by various scientific studies (Bryan and Locke, 1967; Latham and Locke, 1975). In addition to this, there is a myriad of everyday anecdotal experience from the office workspace, which also readily confirms this. Parkinson's law as such has later been interpreted and formalized by Breton and Wintrobe (1982, 1979) to mean "that, under certain circumstances, the number of principals—top and middle managers—in an organization increases at the same time that the number of its agents and its output decline" (Breton, 1995, p. 435).

It is relevant to note, that Parkinson's law of the multiplication of work not only applies to bureaus of the public apparatus, but, like Down's bureaus, also applies to private sector industries (McKee and Wintrobe, 1993) and to political movements. Breton (1995, p. 435), for example, attributed Hitler's rise to power to knitting a loyal network of collaborators based on the principles of loyalty inherent to Parkinson's law. However, this only implies that the concept of the public apparatus is not an absolute one that refers only to "state"-based public apparatuses, but rather that such apparatuses/networks exist at various levels of society. Nonetheless, one has to consider the crucial difference between private enterprises, in which sources of revenue are rents gained on the market on invested capital, and the public apparatus' informal networks that depend on levied taxes of various kinds, including forced loans and unpaid labor.

1.3 IMMORALITY OF THE PUBLIC APPARATUS

During one of his cabinet meetings [Frederick II of Prussia] asked his finance minister why his treasury was so low when his subjects were paying so much tax. Where was all the money going? To explain the problem, the finance minister asked for a piece of ice. He handed it to the minister farthest from the king. By the time the ice reached Frederick all he received was a wet hand. The lesson the finance minister

> *taught the king ranks in wisdom with the parables of the Bible. Most taxes are consumed by the bureaucracies of the government. It is a wonder Frederick even received a wet hand.*
>
> ***(Adams, 2001, p. 214)***

This section summarizes the many aspects of the public apparatus which have moral implications. The focus is on *corruption*, a multifaceted concept ranging from useful illegality (Luhman in: Walter, 2011, p. 44), beneficial corruption (Bovens and Zouridis, 2002), and mercy to a predatory application of power and control (Evans, 1989).

At the end of this section, three cases of interaction with the public apparatus aim to give the reader a closer view on how state power can cause anger and damage to subjects asking for their rights. The first is an extreme request for public information data that belong in the work domain of media research; the second is the request of a highly qualified migrant to obtain a residence permit; the third is about a fight for lands under restitution that were embezzled by local authorities. These cases are stories from the author's personal experiences with the public apparatus. They are of particular interest, as they happened in Austria and Slovenia, which are EU and OECD member states that, according to the UN, have a very strong political and legal culture (United Nations Development Programme, 2015). Both of these countries have had their experience of state-level corruption—Slovenia has had its scandal on state-level weapons trade during the Balkan war (Frangež, 2007) and the postindependence communist-style privatization period, while Austria was shocked by revelations of predatory party networks' control of a major bank (Kuch, 2011) and the (not uncommon) suspicious privatizations of state property (Mayr, 2011). Such national-level corruption which may involve "old-boy" networks and reach into the formal branches of state power is *part of the game* of the public apparatus and hence a distinct feature, as shall be outlined below.

The eruption of system-level scandals is often no more than a symptom of surfaced wars for dominion over parts of the public apparatus among bureaus or networks. While it may be amusing for the masses to feast on these shocking revelations, they hardly affect[9] how the public apparatus is perceived at large. Nevertheless, personal experiences with the public apparatus that affect the fate, property, or pride of individuals, such as the three

[9]It might perhaps influence their voting behavior, or even more so make them exploitable to mass movement and revolution if fueled appropriately, but a debate on this would exceed the scope of the present treatise.

cases described below, will incite individuals to critically rethink the status quo and open them up to alternatives.

1.3.1 Part of the Game

Corruption is an ever-present feature of human-based government, influencing the accessibility, timeliness, quality, and cost of government. Corruption as part of government is a well-studied topic that is subjectively perceived as a positive or negative factor, depending on the point of view. Colombatto (2003), for instance, aims to explain the positive side of corruption from the perspective of a functioning society. He argues that government corruption is part of the unwritten laws that govern societies, and a factor for balancing interests and keeping social peace, such that it is tolerated in any modern form of government.

Thus, in developed, industrialized countries, widespread corruption takes place at the level of policy-making, as well as through political parties. At the level of policy-making, producers "induce policy-makers to become dependent on illegal income flows. As a result, their behavior becomes more predictable and the transaction costs connected with normal business practice are ultimately reduced" (Colombatto, 2003). Further corruption occurs at the level of political parties, which provide crucial manpower for keeping the public apparatus running. Thus, Colombatto notes, "in many Western European developed countries bribes have therefore become a tolerated—if not outright accepted—instrument to finance a party-controlled institutional framework."

In developed countries corruption takes place in spheres far away from the average person, and is indirectly financed via taxation. Totalitarian and transitional regimes, on the other hand, deploy *street-level* corruption to satisfy the requirements of the public apparatus. In such conditions, civil servants are "offered a minimum, but secure income, and the possibility to make extra money or—more generally—enjoying extra benefits through corruption, conditional upon the benevolence of the ruling class" (Colombatto, 2003).

This form of corruption can be, as Shleifer and Vishny (1993) note, quite fair:

> *In the old-time Communist regimes, and in regions dominated by a single mafia [,] it is always clear who needs to be bribed and by how much. The bribe is then divided between all the relevant government bureaucrats, who agree not to demand further bribes from the buyer of the package of government goods, such as permits. [. . .] Any deviation from the agreed-upon pattern of corruption would be penalized [and] once a bribe was paid, the buyer got full property rights over the set of government goods that he bought.*

Such *monopolistic* corruption is bound to a central authority (such as a party or mafia) that can guarantee stability and fairness. Once such authority is taken out of power, the system collapses and a multitude of independent bribe-takers emerge at various levels of government, each of whom fails to provide the quality and stability as that of monopolistic corruption. For example, this has happened in postcommunist Russia, in many African countries, and in India (Shleifer and Vishny, 1993).

Government corruption is essentially an underground market for property rights. This market exists as governments have the monopoly on assigning, reassigning, modifying, or attenuating property rights (Benson and Baden, 1985). Corrupt officials enable the trade of modifications of such property rights, as they have been endowed with the appropriate discretionary power to create, modify, and destroy *jural relations* (cf. Chapter 6). Needless to emphasize, discretionary power becomes greater as the government regulations become more unclear.

In both developed and developing countries, corruption is thus an important enabler of stability and balance between various interests, an efficient informal mechanism to impose informal policies upon outsiders of the system, and a way to curb competition within the system itself. However, aside from this aspect, corruption remains a burden for those who are involved in mere passive interactions with the public apparatus, or worse, are outsiders to that system.

To create rents for stakeholders profiting from the system, governments, according to Parkinson's law, need to create work and revenue. They do that by imposing new regulations (Shleifer and Vishny, 1993, p. 616) and new forms of taxation. The system of public administration and its dependent stakeholders of the public apparatus thus increases in size, resulting in a complex ecosystem that exists by virtue of the capital available within its reach, such as taxes, labor, and natural resources.

Within the ecosystem of the public apparatus, due to a lack of clear hierarchy, informal networks take control, which Banfield (1975) terms *machines*. These machines are communities, which exist based on a system of exchanges of favors (such as jobs, opportunities to make money by legal or other means, and perks) among officials or external stakeholder groups. Such hierarchies, which "arise from extra-legal, if not illegal arrangements, are ad hoc, and must be continuously renewed by 'deals' in order to prevent them from collapsing" (Banfield, 1975).

Corruption is thus an important factor in stabilizing relations within the society of the public apparatus and helps establish loyalty to organizations or leaders. One might go even so far as to say that corruption is a requirement for the symbiosis of various interest factions that make up the public apparatus. This symbiosis, and hence the peace within, relies on sufficient revenue provided by the governed subjects (by way of taxes or bribes). Accordingly, social peace relies essentially on the sustainability of this symbiosis. Yet, one should ask, as Walter (2011, p. 66) did: "How much more incompetence, thirst for power and excessive costs are we prepared to pay as a price for democracy?"[10]

The excessive demands of the public apparatuses are an everlasting challenge to the stability of any civilization. The limits of the bearable extent of the public apparatus, as manifested through taxation, are easily reached and, as Adams (2001) argues, have caused the dusk of many once strong civilizations, including ancient Egypt, Greece and Rome, the Aztec Empire, and the modern-era European empires. As implied by Adams, the sustainability and success of civilizations lie in the capability of their governance to balance a symbiotic relationship with their subjects, with focus on efficiently providing stability, justice, and freedom.

1.3.2 The Imperfect Human Factor—Fallibility, Incompetence, Ignorance

Aside from institutionalized corruption, far more banal human characteristics play an important role in the stability of the public apparatus: forgetfulness, fallibility, prejudice, incompetence, slowness, etc., of the individual agents who act on behalf of bureaus or the state. Each human involved in decision-making is a potential source of error and a dampening factor in the flexibility and speed of the procedures at stake. As Parkinson argues, the theory of public choice supports (Buchanan et al., 1980; Downs, 1967), and as witnesses continuously confirm (Djilas, 1957; Walter, 2011), many of the hands involved in decision-making in organizations of the public apparatus exist for the sole reason of providing jobs for loyal individuals.

The imperfection of the human action bears significant economic opportunity for rethinking processes and approaches which involve human agents. Weber's model to structure the decision-making processes into a system based on rational-legal authority was all about constraining this human

[10] *"Weber stellte sich 1918 die Frage, wie bei der steigenden Machtstellung des staatlichen Beamtentums Demokratie überhaupt möglich sein wird. Dieses Problem scheint heute gelöst. Heute stellt sich vielmehr die Frage, wie viel 'Unfähigkeit, Herrschsucht und übermäßige Kosten' (Ellwein, 1994, in: Walter, 2011) wir gewillt sind, als Preis für die Demokratie zu bezahlen."*

imperfection. While Weber's theoretical model is hailed by theoreticians for its stability (Olsen, 2006), its crucial reliance on human agents still implies significant flaws. The rigidity of Weberian organizations incites those in power to violate moral principles and stifle moral agency (Adewale, 2017); the nonregulated spheres of discretionary power foster corruption and misuse (Bovens and Zouridis, 2002); and the work culture becomes a hotbed of incompetence, self-sufficiency, and incestuous work ethics (Parkinson, 1955; Walter, 2011).

Rationalizing, structuring, disciplining, and "civilizing" the human factor is part of Western custom, a result of evolution stemming from the age of industrialization. The engineering of machines that depend on human labor to operate and the necessity for them to be kept running constantly (steam-powered machines and furnaces) introduced the concept of regular work shifts, as well as process steps that required a strictly synchronized workforce (Zuboff, 1988). This was the time when the pace of the industrialized Western European culture separated from the daily rhythm of the African, Asian, and even Eastern and South European cultures, which had not yet experienced the tediousness of industrial labor. Even today, "eastern," "southern," or "colored" people in the Western[11] consciousness (as well as among their own ethnic communities) are perceived as stereotypically unreliable, undisciplined, unpunctual, due to their cultural lack of rigidity for certain processes. The notorious *colored people's time* as used in the African and Indian communities (Henry, 1965) or the Muslim *Insha'Allah* ("if God wills") concept remain firm cultural institutions that relativize expectations in business relations with Asian, Middle Eastern, African, or Latin American partners in global business (Meyer, 2014).

Erin Meyer's (2014) *The Culture Map* divides work habits into rigid (thus, reliable) and flexible (hence, unreliable), with the German culture being extremely rigid, punctual, and reliable, and Arabian and African cultures being extremely flexible, fluid, and adaptable. This cultural divide is reflected also in the above-discussed systems of *part-of-the-game* corruption, where Western system corruption occurs in the discretionary spheres of the highest levels of society, while the rest of the world experiences state corruption fluidly at all levels of subject-state interaction.

The manifold challenges of the human factor were also known in the Western world at the brink of industrialization: factory owners struggled to

[11]The *Western* world includes the Germanic, Anglo-Saxon, and Nordic cultures, plus the Japanese culture.

find a workforce, and if they found one, they struggled with their unreliable work ethics, laziness, and incompetence.

> *Attendance [by workers] was irregular; workers would sometimes stay away from the job for days and send for their wages at the end of the week. [. . .] Workers continued to celebrate Saint Monday—a weekly day of leisure spent in the alehouse enjoying drink, bar games, entertainments, 'pugilism,' and animal fights.*
>
> ***(Zuboff, 1988, p. 32)***

Succinctly, the workers worked as much as they needed to survive and feed their families.

> *Nineteenth-century American industrials faced a similar set of problems when it came to honing the worker's body as an instrument of production. The owner of a Pennsylvania ironworks complained of frequent 'frolicking' that sometimes lasted for days, along with hunting, harvesting, wedding parties, and holiday celebrations. One manufacturer filled his diary with these notes: 'All hands drunk; Jacob Ventling hunting; molders all agree to quit work and went to the beach. Peter Cox very drunk and gone to bed. . . . Edward Rutter off a-drinking. It was reported he got drunk on cheese.'*
>
> ***(Gutman (1976) "Work, Culture, and Society in Industrializing America," cited in: Zuboff, 1988, p. 33)***

This inherent utilitarian human laziness is highlighted in an old Upper Carniolan folk song: *"Nedela je bela, pondelk' je pa plav; u tork' se ne dela, u sredo pa mav; četrt'k je rajtnga, u pet'k pa dnar; u zboto pa fajrabnd!"*[12]

While the relations between capital owners and their workforce remain a private matter between the two, this does not hold for the agents of the public apparatus. The performance of these agents impacts the legitimacy of the public apparatus in its entirety and the sentiment of the individual tax residents of the public apparatus' home community in particular. An "honest and hardworking" public apparatus may uphold an aura of trust and rational legitimacy, such being the case, e.g., in Switzerland, Norway, or Germany (OECD, 2015, chap. 11), while the perception of inefficiency and corruption will render a national public apparatus vulnerable to instability, foreign takeover, and chaos, inciting the home community to tolerate emerging structures of power, as transpired in the Arab Spring or the Iranian revolution.

It goes without saying that the vulnerability of existing structures of power opens up an assortment of opportunities for challengers and transformation. Bureau-level vulnerabilities enabled the creation of the CIA,

[12] "The Sunday is white (holy), and Monday is blue (off); on Tuesdays one does not work, on Wednesdays only a little bit; on Thursday one issues the bill, on Friday one gets paid; on Saturday finally comes the after-work party!"

which grew and invaded the turf of the US State Department (Downs, 1967, p. 215); similar vulnerabilities also enabled the coexistence of two significant armed forces in Lebanon—the government's Western- and Saudi-backed Lebanese Armed Forces and the Iran-backed Shiite Hezbollah. In a similar fashion, European political parties post-WWI developed their private intelligence and military forces (such as Hitler's SA "Brownshirts" or Mussolini's "Blackshirts") behind the backs of vulnerable states. These forces later engaged in civil-war-like street warfare until the Nazis in Germany and Fascists in Italy emerged as the dominant powers.

1.3.3 Case One: Inefficiency—Access to Public Information

Inefficiency in dealing with unexpected situations is hazardous to a bureau's integrity, as it can clog up the bureau's normal workflow, make it seem vulnerable, or even paralyze it. In the constant struggle for resources and stable dominion within the public apparatus, bureaus, networks, or paradigms showing signs of weakness may easily fall prey to competitors who consider themselves better suited to address the situation which the others have failed to resolve. The following is a summary of a case (Paulin, 2010) of such inefficiency that unveils existing vulnerabilities which could be exploited by competing networks.

In summer 2010 requests were made to more than 350 Slovenian public legal entities (ministries, municipalities, local administrative units, universities, etc.) to provide the names, total remuneration received, and full work reports of each of their employees for the year 2009. According to Slovenian law,[13] state-held information is public (and hence access must be granted) if the requested information is about public spending, or public employees, among other reasons. From a technological perspective, this information could easily be made available for self-service access, just as one would access information about an office's opening times, the names of the members of parliament and city councils, parliamentary debates, the government's annual budget, or court cases of the higher courts.

Each of the over 350 agencies were contacted through automated freedom of information requests by e-mail. The e-mail addresses were collected from Slovenia's central catalog of public information (the CKIJZ[14]), established by the *Ministry for Public Administration* in accordance with a 2007 decree.[15]

[13]Zakon o dostopu do informacij javnega značaja (Public Information Access Act), EVA 2002-2811-0001.

[14]*Centralni katalog informacij javnega značaja*, http://www.ckijz.gov.si.

[15]EVA 2005-3111-0008.

In summer 2010, the CKIJZ listed 863 public organizations. There are more public organizations than that in Slovenia, though the exact number is not documented—the lower courts were missing entirely and only 165 out of 210 municipalities were listed. From the listed organizations, 152 listings were dead, 190 did not provide contact information, and 15 provided dead e-mail contacts. In 2016, the CKIJZ was offline, even though the *Information Commissioner*'s (the agency responsible for governing the access to public information and data privacy domains) web page still linked to it.

This massive request soon stirred up a buzz, driving the *Information Commissioner* to issue a general recommendation that the request *must* be granted. The *Ministry of Finance* (which ultimately processes the public employee's payslips) developed a software solution (a database template) to extract the requested data on a per-agency basis and sent reports to the agencies upon request. Several of the addressed organizations disputed the validity of the request and some of them engaged in legal disputes, or pretended the request was unspecific, or similar. Organizations which put up a legal struggle against the request included all of the highest authorities of statehood—the *Constitutional Court*, the *National Council* (the lower chamber of the Parliament), the *Office of the State Prosecutor General*, and the *Faculty of Law of the University of Ljubljana*, Slovenia's most significant university in the field of law.

The entire operation wasted an uncountable amount of labor on the side of the public apparatus. One agency, an employer of roughly thousand employees, estimated it would take them at least 20 hours of work to collect the requested data. With about 160,000 public employees, that would hypothetically amount to 24 full man-months of work. Though the request was an isolated case without much of an ulterior motive, if scaled up and orchestrated properly, such requests could easily be used for denial-of-service (DoS) attacks on agencies of the state.

The DoS attack is a well-known type of attack against technical systems, in which a system is flooded with requests until it collapses. This tactic is not limited to attacking technical systems: The Scientology vs. the US Internal Revenue Service (IRS) war for tax exemption (Owen, 1998), in which the Scientology organization brought the IRS to their knees, is a standout example of a modern organization-level DoS attack. Another modern example is the 2015 European migration crisis in which over a million Central Asian and Middle Eastern migrants marched over the borders of Hungary and former Yugoslavia. Their desire to settle down under refugee status in Germany, the United Kingdom, or the Nordic countries led to a collapse of the border regimes and a standstill of the Budapest–Munich train itinerary.

Unlike the Scientology vs. IRS conflict, the European migrant situation is likely not centrally orchestrated, but evolved naturally into a complex economy of actions and interests of NGOs, political actors, smugglers, entrepreneurs, war agents, "terrorists," or other interest groups expecting gain from changing circumstances, instability, or new business opportunities.

System vulnerability, or suboptimal performance, reveals opportunities for competitors to emerge and take over a business. If the right to public data is to be enforced with due diligence, then the only sustainable and efficient way to enforce it is to deploy technological solutions to circumvent human decision-making in accessing the data. Circumventing the human factor is necessary in achieving this goal—while humans assume a gatekeeper role, they may prioritize their private interests or the interests of their organization over the rights of the information seeking party.

In the above-described case from Slovenia, the bureaucratic approach (in Weber's sense) made the freedom-of-information requests costly to process. Not only did it incur easily avoidable costs from the part of human labor, but it also provoked a feeling of discomfort and unease for the information seeker, who was forced into situations of conflict with government agencies.

1.3.4 Case Two: Sluggishness—Request for a Residence and Work Permit

The second case is a request for a residence permit which was observed in autumn 2012 in Vienna, Austria. The applicant, a citizen of a non-EU state, requested a residence and work permit, which was required in the case of employment as an academic researcher. Austria encourages the immigration of highly qualified people, and hence the law mandates that valid requests shall be granted *immediately* (unverzüglich), or at latest within 8 weeks (i.e., 56 days) from the date of application.

The application has to be filed at an Austrian embassy, which instantly rejects incomplete applications. Complete applications are received (in the case of Vienna) by the municipality, which must—*without hesitation* (unverzüglich)—request that the *National Employment Service* (AMS) provide confirmation that the applicant may be accepted to enter the job market. If the confirmation has been provided, the municipality grants the request and issues the residence permit. In order for the applicant to collect this residence permit, they must then apply for another visa dedicated to this sole purpose.

In the observed case, the applicant was aided by a legal representative, who monitored the proceedings and undertook significant effort to expedite the process, including frequent (sometimes daily) telephone calls to all responsible officials, e-mail petitions urging speeding up of the process, personal visits, and complaints to supervisors. Despite this, the proceedings took significantly longer than mandated by law, but was nonetheless processed in record time in comparison to similar cases. During interactions with lower-level officials, the applicant and their representative were treated in an unwelcoming and disrespectful manner, and the officials demonstrated strong ignorance toward the provisions of the law. When reminded about the law's provision to complete the proceeding within 8 weeks at latest, a manager-level official responded: "So what? Then come back in 8 weeks and file a complaint!"

In this case, there were only two points at which decisions had to be made by officials: first, by the embassy when the request was filed, where it could have been rejected immediately as an unqualified request; and second, at the AMS, whose task was to examine the case and who could reject the application if the conditions for entering the Austrian job market were not fulfilled. It took the AMS less than 1 week to decide; the rest of the time (at least 80 days) was spent in transit or with the file lying idle.

Unnecessary delays like these have become hard to comprehend, as many components of the world we live in are now so easily and quickly accessible to us. Sluggish administrative proceedings coupled with derogatory behavior leave a bad impression and easily destroy the illusions of a virtuous and efficient administration. It is such intensive experiences with the brutishness of the public apparatus which make individuals open to reform.

1.3.5 Case Three: Predatoriness—Embezzled Lands

In the years following the declaration of independence from Yugoslavia, Slovenia passed denationalization laws, which aimed to restitute property seized by the state during the country's socialist era. Immediately after the socialist revolution during WWII, the property of so-called capitalists, land owners, and other wealthy citizens were systematically expropriated in several waves of nationalization. In 1945, immediately following the war, property was seized by means of dubious court trials in which wealthy citizens were accused and convicted for alleged crimes against society, such as "attempts to sabotage forthcoming property reforms." The first expropriations based on passed laws were conducted in

1946, based on the *agrarian reform*, in which all farm lands exceeding a certain size were seized. In 1948, traders and entrepreneurs were expropriated, seizing shops, cooperatives, and businesses. Finally, in 1958, rental apartments and urban lands were nationalized.

The denationalization law of 1992 aimed to restitute the seized property, either by returning the previously nationalized real estate in kind, i.e., returning the real estate as such to the heirs of the previous owners, or by giving a substitute in the form of government bonds, though these were merely symbolic in comparison to the real market value of the seized properties. The denationalization law[16] (ZDen) declared in §88 the real estate, on which claims for restitution were made, as *rei extra commercium*, i.e., forbidding any kind of disposal (such as trade) until the restitution claims were decided to be legally binding.[17] At the same time, ZDen §32/II provisioned that land on which real estate has been built shall not be returned, unless the hovering real estate is property of the original owner.[18] The separation of land (*fundus*) and the hovering real estate (*object*) was necessary, since the Yugoslavian ZTLR,[19] which was valid until 2002, supported a separation in ownership between land and building. The Slovenian SPZ[20] later introduced the principle *superficies solo cedit*, making the building *part of* the land.

Despite being exempt from disposal by law, a significant amount of lands that were still in the possession of the state were sold by municipalities (who were formally still the owners). The observed case involved more than 25 construction lots for family houses and one large lot for a retirement home, which the Prebold municipality sold between the years 2004 and 2006 to private buyers who went on to construct family houses on these lots. When the heirs of the denationalization beneficiary discovered the constructions and confronted the municipality, the latter arrogantly assumed the position that the

[16] *Zakon o denacionalizaciji* (Denationalization Act, ZDen), SOP 1991-01-1094.

[17] *"(I) Z dnem uveljavitve tega zakona ni dopustno nobeno razpolaganje z nepremičninami oziroma premoženjem, glede katerega po določbah tega zakona obstaja dolžnost vrnitve. (II) Pravni posli in enostranske izjave volje, ki so v nasprotju s prejšnjim odstavkom, so nični."*

[18] *"(II) Podržavljena zazidana stavbna zemljišča (obstoječe gradbene parcele) se ne vračajo, razen če je na njih zgrajeni trajni objekt v lasti upravičenca."*

[19] *Zakon o temeljnjih lastniškopravnih razmerjih* (Basic Property Law Relations Act, ZTLR), SOP 1980-07-0088.

[20] *Stvarnopravni zakonik* (Law of Property Code, SPZ), SOP 2002-01-4360.

heirs will get the substitute government bonds in any case, and so they should not make a fuss around the matter.

The heirs took legal action by suing the municipality to declare the sales void and pressed corruption charges against the mayor. Though the state prosecutor found evidence for criminal activity, the charges were dropped under the statute of limitations. In the same year, the court of first instance dismissed the cases. The reasoning followed the argumentation of the municipality, which brought forward that the lands must not be returned, since (given that the buildings were already constructed) ZDen §32 applies, and hence, the denationalization beneficiary is only entitled to the substitute bonds. This decision was contested by the plaintiff; the court of second instance upheld this appeal, rejected the opposition, and rolled back the contracts from 2005 to 2007.[21]

In Slovenian legal practice, a conflict between ZDen §32 and §88 has formed, whereby claims aiming to nullify sales in accordance with §88 were rejected if meanwhile a final decision has been reached that §32 applies,[22] i.e., by the mere circumstance that buildings have been constructed. In such a case, the restitution of the nationalized property was made in the form of government bonds for an amount which was often less than 1% of the market value, and often far less than even the costs of the legal proceedings. On the other hand, as long as the denationalization case was still pending, §88 applied unconditionally.[23]

This predatory behavior of networks ruthlessly exploiting their power in their particular domain of the public apparatus is particularly damaging to the latter's integrity and invokes anger, injustice, and distrust in the stakeholders involved. Such predatory agents gradually change the culture of the public apparatus from a synergetic relationship in which the actors enjoy legitimacy and trust to a parasitic one in which the public apparatus actors systemically usurp the available resources in one form or another. In the described case, the 2004–2006 land deals were engineered by the municipality's lawyer, who also represented the defendants during the legal proceedings. Even though he lost all cases without exception, this lawyer "earned" himself a decent income ultimately paid out of the municipality's budget.

[21]Higher Court Celje, VSC Cp 426/2015.
[22]Supreme Court, VSRS X Ips 80/2013.
[23]Constitutional Court, U-I-95/91, later reconfirmed by Up-195/00.

REFERENCES

Adams, C., 2001. For Good and Evil: The Impact of Taxes on the Course of Civilization, second ed. Madison Books, Lanham, MD.

Adewale, A., 2017. Does bureaucracy stifle moral agency? Int. J. Public Adm. Digit. Age 4, 1–13.

Albrow, M., 1972. Bürokratie. List-Taschenbücher der Wissenschaft Politik. List, München.

Amanat, A., 2011. Ebrāhīm Kalāntar Šīrāzī. Encyclopædia Iranica. Columbia University, New York.

Anderson, B.R.O., 2006. Imagined Communities: Reflections on the Origin and Spread of Nationalism, revised ed. Verso, London, New York.

Bajt, A., 1999. Bermanov dosje, Zbirka Premiki. Mladinska knj, Ljubljana.

Ballantyne, B., Bristow, M., Davison, B., Harrington, S., Khan, K., 2000. How can land tenure and cadastral reform succeed? An inter-regional comparison of rural reforms. Can. J. Dev. Stud. 21, 693–723. https://doi.org/10.1080/02255189.2000.9669909.

Balut, A., Cabada, L., 2000. Post-komunistične stranke—primerjava razvoja Zveze komunistov Slovenije in Komunistične stranke Češkoslovaške[Post-communist political parties—comparing the development of the League of Communists of Slovenia and the Communist Party of Czechoslovakia]. Teorija in praksa 37, 749–766.

Banfield, E.C., 1975. Corruption as a feature of governmental organization. J. Law Econ. 18, 587–605.

Bannister, F., 2017. In defence of bureaucracy: governance and public values in a digital age. In: Paulin, A.A., Anthopoulos, L.G., Reddick, C.G. (Eds.), Beyond Bureaucracy. Springer International Publishing, Cham, pp. 27–47. https://doi.org/10.1007/978-3-319-54142-6_3.

Benson, B.L., Baden, J., 1985. The political economy of governmental corruption: the logic of underground government. J. Leg. Stud. 14, 391–410.

Boduszynski, M.P., 2000. Triumph of the opportunists: the political rebirth of ex-communists. Newsletter of the Center for Slavic and East European Studies 17, 3–9.

Bovens, M., Zouridis, S., 2002. From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control. Public Adm. Rev. 62, 174–184. https://doi.org/10.1111/0033-3352.00168.

Brecht, B., 2003. Wenn die Haifische Menschen wären. In: Geschichten vom Herrn Keuner, Bibliothek Suhrkamp. Suhrkamp, Frankfurt am Main.

Breton, A., 1995. Organizational hierarchies and bureaucracies: an integrative essay. Eur. J. Polit. Econ. 11, 411–440. https://doi.org/10.1016/0176-2680(95)00011-L.

Breton, A., Wintrobe, R., 1979. Bureaucracy and state intervention: Parkinson's law. Can. Public Adm. 22, 208–226. https://doi.org/10.1111/j.1754-7121.1979.tb01813.x.

Breton, A., Wintrobe, R., 1982. The Logic of Bureaucratic Conduct: An Economic Analysis of Competition, Exchange, and Efficiency in Private and Public Organizations. Cambridge University Press, Cambridge.

Bryan, J.F., Locke, E.A., 1967. Parkinson's law as a goal-setting phenomenon. Organ. Behav. Hum. Perform. 2, 258–275. https://doi.org/10.1016/0030-5073(67)90021-9.

Buchanan, J.M., Tollison, R.D., Tullock, G., 1980. Toward a Theory of the Rent-Seeking Society. Texas A&M University Economics Series, vol. 4. Texas A&M University, College Station.

Castells, M., 2010. The Rise of the Network Society, second ed. The Information Age: Economy, Society, and Culture. Wiley-Blackwell, Chichester, West Sussex; Malden, MA.

Colombatto, E., 2003. Why is corruption tolerated? Rev. Austrian Econ. 16, 363–379.

Cungu, A., Swinnen, J.F.M., 1997. Agricultural privatization and decollectivization in Albania: a political economy perspective. In: Swinnen, J.F.M. (Ed.), Political Economy of Agrarian Reform in Central and Eastern Europe. Ashgate, Brookfield, VT.

Djilas, M., 1957. The New Class—An Analysis of the Communist System. Thames & Hudson, London.
Downs, A., 1967. Inside Bureaucracy, A Rand Corporation Research Study. Little, Brown, Boston, MA.
Dzero, A., 2011. Contemporary Russian Identity and the Soviet Union: Continuity and Confrontation. The University of Sydney, Sydney.
Evans, P.B., 1989. Predatory, developmental, and other apparatuses: a comparative political economy perspective on the third world state. Sociol. Forum 4, 561–587. https://doi.org/10.1007/BF01115064.
Frangež, M., 2007. Kaj nam pa morete!: od trgovine z orožjem do Depale vasi [You can't do nothing against us! From the weapons trade to the Depala vas scandal]. Matjaž Frangež, Ljubljana.
Graeber, D., 2015. The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy. Melville House, Brooklyn/London.
Gutman, H., 1976. Work, Culture, and Society in Industrializing America: Essays in American Working-Class and Social History. Alfred A. Knopf, New York.
Habermas, J., Burger, T., 2008. The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society, reprinted ed. Polity Press, Cambridge.
Henry, J., 1965. White people's time, colored people's time. Society 2, 31–34. https://doi.org/10.1007/BF03180813.
Jellinek, G., 1905. Allgemeine Staatslehre. In: Das Recht des modernen Staates. Verlag von O, Härig, Berlin.
Kranjc, J., 2015. The Illyrian provinces and the reform of territorial administration. Lex localis—J. Local Self-Gov. 13, https://doi.org/10.4335/13.1.59-78(2015).
Kuch, K., 2011. Land der Diebe [Land of Thiefs]. Ecowin Verlag, Salzburg.
Kurzman, C., 1996. Structural opportunity and perceived opportunity in social-movement theory: the Iranian revolution of 1979. Am. Sociol. Rev. 61, 153. https://doi.org/10.2307/2096411.
Latham, G.P., Locke, E.A., 1975. Increasing productivity and decreasing time limits: a field replication of Parkinson's law. J. Appl. Psychol. 60, 524–526. https://doi.org/10.1037/h0076916.
Lemel, H., 1998. Rural land privatisation and distribution in Albania: evidence from the field. Eur. Asia Stud. 50, 121–140. https://doi.org/10.1080/09668139808412526.
Mayr, W., 2011. Corruption Scandals in Austria: A Web of Sleaze in Elegant Vienna. Spiegel Online, Hamburg.
McKee, M., Wintrobe, R., 1993. The decline of organizations and the rise of administrators. J. Public Econ. 51, 309–327. https://doi.org/10.1016/0047-2727 (93)90068-5.
Meyer, E., 2014. The Culture Map: Breaking through the Invisible Boundaries of Global Business. PublicAffairs, New York.
OECD, 2015. Government at a Glance 2015. OECD Publishing.
Ogden, D., 2013. Drakōn: Dragon Myth and Serpent Cult in the Greek and Roman Worlds, first ed. Oxford University Press, Oxford.
Olsen, J.P., 2006. Maybe it is time to rediscover bureaucracy. J. Public Adm. Res. Theory 16, 1–24. https://doi.org/10.1093/jopart/mui027.
Owen, C., 1998. Scientology Versus the IRS [WWW Document]. https://www.cs.cmu.edu/~dst/Cowen/essays/irs.html. (Accessed 31 January 2016).
Parkinson, C.N., 1955. Parkinson's law. The Economist.
Paulin, A., 2009. Zwischen Scylla und Charybdis—Aufstieg und Fall einer Oberkrainer Bürgerfamilie [Between scylla and charybdis—Rise and fall of an Upper Carniolan upper-class family]. Carinthia I 199, 691–698.
Paulin, A., 2010. Slovenia 404—on the e-readiness of modern public administration. In: Proceedings of the International Conference on Information Society and Information Technologies. Faculty of Information Studies, Dolenjske Toplice.
Rebel, H., 1983. Peasant Classes: The Bureaucratization of Property and Family Relations Under Early Habsburg Absolutism. Princeton Univ. Press, Princeton, NJ, pp. 1511–1636.

Robisheaux, T.W., 2002. Rural Society and the Search for Order in Early Modern Germany, paperback ed. vol. 1. Cambridge University Press, Cambridge.

Shleifer, A., Vishny, R.W., 1993. Corruption. Q. J. Econ. 108, 599–617.

Trnavci, G.H., 2008. The Albanian Customary Law and the Canon of Leke Dukagjini: A Clash or Synergy with Modern Law. ExpressO.

United Nations Development Programme (Ed.), 2015. Work for Human Development, Human Development Report. United Nations Development Programme, New York, NY.

Walter, A., 2011. Das Unbehagen in der Verwaltung: warum der öffentliche Dienst denkende Mitarbeiter braucht [The Apprehension of the Administration—Why the Civil Service Requires Staff That Thinks]. Edition Sigma, Berlin.

Wysling, A., 2015. Tricksende Südeuropäer—Warum sie ihre Steuern nicht zahlen [Cheating South Europeans: Why They Don't Pay Their Taxes]. NZZ Mediengruppe, Zürich.

Zuboff, S., 1988. In the Age of the Smart Machine: The Future of Work and Power. Basic Books, New York.

CHAPTER 2

Digitalized Governance—An Embezzled Opportunity?

Contents

The evolution of the public apparatus, as discussed in Chapter 1, is foremost a matter of opportunity. Opportunity, then, needs to be approached, embraced, and seized. The most basic opportunity for the emergence and expansion of a public apparatus is the protection of property, then comes social care, then culture (arts and science), and finally, unrestrained stakeholder expansion, that is the *withering away of the state*[1]—i.e., the replacement of a clear formal bureaucracy for a public apparatus that includes everyone and everything (Chapter 5 explores further the life cycle of the public apparatus). With the advent of informatics, new opportunities arise for the public apparatus to reorganize, expand, or transform by means of the digital domain.

First, informatics has enabled new opportunities for surveillance and espionage (video surveillance, satellites, face recognition, surveillance of monetary flows, sentiment surveillance, etc.), which offer an expansion of the

[1]"Withering away of the state" is a Marxist concept, coined by Friedrich Engels in his book *Anti-Dühring.* In this treatise, it is used as a paraphrase. Engel's original concept referred to the state machinery ceasing to exist as it becomes superfluous due to advances in technology and society.

https://doi.org/10.1016/B978-0-12-816224-8.00002-9

public apparatus into domains that previously simply did not exist. A whole new ecosystem of activities and opportunities to create work emerges from technicized surveillance alone: protection of privacy, information governance, biometrics, computer vision, etc. Expansion into these novel domains can be legitimized by arguing public safety (think: terrorism, prevention of pandemics, surveillance of crime, …), when often it boils down to forms of domestic control (oppression of dissidents, prevention of tax evasions, manipulation of the public opinion, etc.).

There is then the opportunity for an internal "housecleaning" of established bureaus. Tech-savvy networks (or bureaus) find their chance to seize control by reengineering processes, introducing new technology for tasks of back and front offices alike. They undermine existing power relations by creating a dependency on the newly introduced technology that is under their sole control. This wave of modernization reshuffles and outdates the traditional bureaucratic hierarchies and allows for new players to enter the stage in an often wild and uncontrolled manner under the pretext of reducing costs in the public administration, speeding up processes, and reducing "red tape."

The third is the opportunity for the inclusion of new stakeholders into the public apparatus, and the withering away of the borders between the state and its people. This is a point in which modern expectations of citizen participation, citizen deliberation on public matters, coproduction based on government data, and participatory governance reach rather unsubstantiated dimensions (to be discussed in Section 2.2, from the perspective of governance technology, and later in Section 3.5, from the perspective of democratic participation).

We aim to resolve this throughout this book: While the status quo of digitalization (a critique of which is outlined in this chapter) has yielded a chaotic, ad hoc, fragmented, feudalistic, uncontrollable, and unsustainable approach to modernize public governance, this book aims to develop a systemic, controllable, and sustainable technological base framework. Just as the metric system was able to bring order to the myriad of medieval measuring systems, this book aims to develop a universal systematics for developing technology for governance.

As a gentle introduction to the topic, Section 2.1 aims to provide an overview over the buzzwords that emerged as marketing vehicles during the past decades in public discourse, industry, and academia, such as e-government, e-governance, e-democracy, e-participation, open (government) data, smart city, and smart governance.

2.1 THE BUZZWORDS AND WHAT THEY ARE ALL ABOUT

With the extensive hype for the WWW from the late 1990s to deep into the second decade of the 21st century, the public conscious has been flooded with vivid new buzzwords aiming to rehash, repackage, and oversell the very simple and natural introduction of information and communication technologies (ICTs) into the context of public service delivery. First, it became fashionable for governmental agencies to become *digital* (in the US), or *electronic* (everywhere else), *mobile*, and finally *smart*. The evolution of the name, however, neither reflected radical transformations, nor did it trigger them.

These buzzwords remained, born out of publicity jargon. Much like the term *bureaucracy* grew from casual use to scientific terminology (Albrow, 1972), these buzzwords rose from the shabby marketing milieu to the ivory towers of science, sparking dedicated academic conferences and journals.

Grönlund and Horan (2005) attempted to chronicle the beginnings of *e-Gov*—an umbrella term encompassing e-government, e-governance, digital government, one-stop government, and online government. They find its roots in the late 1990s, when practitioners engineered solutions to introduce the emerging Web technology into the manifold facets of the public apparatus. As the name suggests, the focus of these endeavors was the Web-ization of government, or more specifically its citizen-facing channels of communications. The novelty brought about by e-Gov was the *channel choice* (Reddick and Turner, 2012), i.e., the objective that citizens should be offered access to information (on/about government) *online*, hence through the Web.

The fundamental point when considering e-Gov is that there is no underlying systemic approach, neither with regard to technology, nor with regard to legislation or organization. This section aims to provide a simple overview of the terminology; a critique of this lack of systematics is given throughout this book as a whole.

2.1.1 Before e-Gov: Verwaltungsinformatik

Technization of the public apparatus was explored in the decades before the boost brought about by the Web. The widespread use of computers and information systems by governance agencies was observed and studied as far back as the 1970s (cf. Grönlund and Horan, 2005, p. 714). However, at that time, trends to technicize the public apparatus focused on engineering and reengineering back-end systems for professional use and interbureau communication. For example, in the mid-1970s, there was a trend to establish shared electronic databases (Lenk, 2004, p. 91). It was a time in which the emerging information technology and the rapid progress of computer hardware opened up economic opportunity for tech-savvy bureaus to emerge and expand their domains into the realm of competitors.

The Danish *Central Citizen Registry* (CCR), which was developed and implemented during the late 1960s as one of the first (if perhaps not *the* first) central citizen repository worldwide (Zinner Henriksen, 2012), is one such example of e-Gov. The CCR introduced a unique citizen identifier and presented a solid central foundation that survived (with modernizations) well into the 21st century. The knowledge gained with the CCR was exported to Hong Kong in 1975 to build a similar system, which, however, failed as the population was using different calendar systems to indicate their birth, etc. What allowed the Danish CCR to survive for decades was its authoritative approach, its unfussy architecture, and its status as a single entry point to all citizen data in Denmark. The story of the CCR, however, is also a story of a technologically advanced network transforming the Danish public apparatus' established competences, which led to lasting tensions, especially in relation to the Church of Denmark, which thus lost its superior position in registering citizens (Zinner Henriksen, 2012, p. 18).

Before e-Gov, which placed the citizen-user in the spotlight of attention, the focus on professional systems allowed, in the German cultural sphere, for the emergence of *Verwaltungsinformatik*—administrative informatics (Lenk, 2004), a field which attempts to connect the domains of informatics and administrative sciences. *Verwaltungsinformatik* allowed professionals and academics to better understand the challenges in administrative sciences and to use this to focus on knowledge-based systems (recommender systems), governmental databases like the Danish CCR, digital telecommunications, tax systems, business process reengineering, and the like.

Verwaltungsinformatik remains alive in the 21st century, though the focus of the global research communities has shifted toward novel terms in the scope of e-Gov. The hyperinflation of new marketing terms, which entrap researchers and funding agencies in a competition for fabricating new output without new content, is, however, preventing a much-needed maturation of the field.

2.1.2 The Four Stages of e-Gov Maturity

Engineering efforts to reach e-Gov have been considerably low, with the primary result being nothing more than the implementation of an online presence. Research endeavors in this area have been led by social, administrative, and political sciences, which have explored the uptake of these sites (Reddick and Turner, 2012) or their maturity with regard to sophistication (Layne and Lee, 2001). While social science is *observational* in its nature, technical sciences are about creating and evolving *design* (Hevner et al., 2004). Input from thinkers from the technical milieu came in the form of suggestions for systemic organization such as the *one-stop-shop* idea (Wimmer, 2002) that all government services should be accessible through one online endpoint or the *government as a platform* (O'Reilly, 2010)—which advocated that public administration should become open for online peer-production (a bastardized version of this vision had a later revival as part of open government data (OGD) movements).

In its core, the e-Gov paradigm stretched along several models (stages, phases) of maturity (complexity) (Baum and Di Maio, 2000; cf. Layne and Lee, 2001; in: Veit and Huntgeburth, 2014, p. 11); Coursey and Norris (2008) provide a good overview in this regard. The basic stage is a simple Web presence in which information such as description of functions offered by the agency, names of the officials in charge, contact details (phone, e-mail) is provided. This stage was adopted swiftly in the mid-1990s following the advent of the Web and the rapid adoption of the Web browser. The second stage is the interactive stage, in which the Web presence offers interaction, such as providing forums to post messages (two-way communication) or where administrative forms can be downloaded online, to be filled in from home. Little is exciting about this stage neither from a conceptual perspective, nor from an engineering perspective, but it provides considerable added value in the administrative processes, as it facilitates one's acquisition of administrative forms.

The third stage is the *transactional* stage, in which administrative processes can be conducted online. At this stage, one is able to file their tax returns online, prolong their car registration, register change of address, obtain extracts from the land register (or even make a land registration online), view cadastral data, and the like. Unlike the previous two, this stage is both an engineering and, even more so, an organizational challenge, since it requires substantial reorganization of back offices and a complex technization of back-end systems. At this stage, a power shift happens toward tech-savvy bureaus (or networks within), which take over dominions that would have followed strict conservative patterns of operation for decades if not centuries. These conservative patterns are replaced by computerized systems, through which users of these systems interact. This way, the shift toward the fourth stage, that is, the *transformational* stage, of e-Gov happens, which is about process reengineering, interconnected databases held by different bureaus, the digital identity, and so on.

The latter two stages call for an extensive digitalization of the processes required to deliver specific social functions (such as maintaining the land register or providing car insurance) to such an extent that human interaction in handling a case is (at least from a technological perspective) no longer required on the side of the social function provider. (This applies to the fourth stage; the third stage will often include manual handling of cases at the bureau.) These two stages also bear significant engineering, and to some extent even scientific (technical sciences), challenges that involve addressing issues such as standardization of data structures, engineering of protocols for data exchange, and cryptographic challenges, such as those involved with the digital signature or nonrepudiable message exchange (cf. Paulin and Welzer, 2013).

2.1.3 e-Democracy, e-Participation, e-Voting

With the introduction of an online channel for citizens to choose from, e-Gov introduces the concept of *e-Participation*, which in essence is about engaging stakeholders through online forums, online petitions, and the like. e-Participation is, however, slightly different to the broader concept of e-Democracy. How exactly do they differ? For example, when stakeholders are invited to give their opinion on new municipal services or planned changes in the urban environment, it would be called *participation*; if, on the other hand, stakeholder engagement is enriched with decision-making power to decide on public policy, budgetary issues, and so on, then this would then fall under *democracy*. e-Democracy is a field concerned with facilitating inclusion of subjects into political decision-making, which it does through techniques of e-Participation (for purposes of counseling, etc.), and e-Voting.

Technicized voting processes that involve modern telecommunications emerged comparably early. Since the 1970s computer-aided solutions have explored the opportunity to enhance and modernize the processes of voting (Lippert and Ojumu, 2008). e-Voting is based on two main considerations: first, that utilizing ICT will encourage young voters to take part in the elections; second, that the digitalization of the voting process promised a cheaper process and faster results. Voting technology comes in a broad range: in its simplest form, it is about the counting of cast votes, or other structured information such as census data, and dates back to the 19th century. Computers based on Herman Hollerith's 1890 electronic counting machine were used by the US Census Bureau as far back as the 1940s (Gauthier, 2008).

The advent of the Web brought the opportunity to thoroughly modernize e-Voting by utilizing the online channels available. Several real-world experiments featuring e-Voting have been conducted in the mid-2000s—among the first being the US *Secure Electronic Registration and Voting Experiment* in 2004 and the British local elections in 2007, while Estonia implemented e-Voting in political elections continuously on various levels from 2005 onward. e-Voting, however, is limited in its transformational power to the democratic process, as, in essence, it is merely mimicking well-established absentee voting—instead of casting one's absentee vote by mail, e-Voting offers casting it online.

Implementing electronic elections into existing legal and bureaucratic structures was found to be neither cheaper, nor faster (Jones, 2000). In addition to this, several electronic voting experiments have failed to gain public trust in technology due to hazy implementations, naive errors, or even fraud (Kitcat and Brown, 2008; Lippert and Ojumu, 2008; Oravec, 2005; Stokes, 2007).

e-Participation became a prominent and enduring concept due to significant PR backing by civil society activists. The concept of e-Participation is closely linked to the cases of the German Pirate Party's direct democracy system (cf. Section 3.5), the much-hyped Icelandic *crowdsourced* constitution, and a wave of national e-Participation systems like the Estonian 2001-launched *Tana Otsustan Mina* ("today I decide," TOM) (cf. Kitsing, 2011), which give citizens the option to make suggestions for new public policies or laws. By implementing ICTs into the legislative processes, the public apparatus aimed to strengthen its legitimacy in the eyes of young, tech-savvy citizens:

> *e-Democracy can also be seen as a response to declining levels of political participation and decreasing public trust that undermine the legitimacy of democratic institutions. Instead of joining traditional political parties, citizens are seeking out organizations and groups that are more tailored to their specific political interests. [e-Democracy] can also be seen as an attempt to make old-fashioned, non-Internet based (without e-) institutions and structures survive in an e-society.*
>
> ***(Mikaelsson and Wihlborg, 2011)***

In practice however, e-Participation is a rather desolate field. In Slovenia, for example, in 2009 the government set up the online forum *predlagam.vladi.si* (PVS; "I suggest to the government"), through which citizens were invited to propose their ideas and feedback to the government, who in turn promised to have a look at the submissions on which at least 5% of all registered users had voted in favor (Paulin, 2010a). Later, this threshold was lowered to at least 13 votes in favor. As of March 2010, among the five most popular causes on PVS was an appeal to lower VAT on children's diapers—it received 15 comments and 39 votes. By August 2013, PVS had about 2500 suggestions posted in total. One of the very few notable popular items of discussion was a 2011 petition against new legislation that aimed at prohibiting do-it-yourself construction, which received 984 votes in favor and 140 comments. This petition, however, was rejected by the government as "unfit for further consideration" (MiranN, 2011). PVS was essentially a copy of the Estonian TOM, which, though having several thousand registered users, in 2004 had an active population of only a handful "famous freaks, that are trying to start new laws" (Charles, 2004). TOM was later embedded in a succeeding e-deliberation initiative, *osale.ee*, but was continued to be used by an insignificant number of citizens (Kitsing, 2011).

With the aim to motivate their citizens to participate in political processes, Botkyrka, a Swedish municipality, set up a Web forum on which registered users could initiate and discuss political issues of their own choosing. As in the cases of PVS and TOM, local leaders promised to include the online debate into their politics. The forum, however, remained de facto dead:

> *The number of initiated discussions under the forums designated for discussion about issues concerning different municipal areas varies. The forums of some municipal areas have no initiated discussion at all while others have over four-year period generated between 5-10 initiated discussions. About half of all discussions have been initiated by forum moderators or by local politicians. The other half of the discussion has been initiated by users but one single user has initiated most of them.*
>
> ***(Mikaelsson and Wihlborg, 2011, pp. 87–88)***

Another example of e-Democracy in action is the case of Iceland's "crowdsourced"[2] constitution (Morris, 2012), which has been enthusiastically hailed as a bright exception to the many failures of e-Democracy.

Between 1998 and 2003, nationally held banks in Iceland were privatized, apparently without proper care, which left the second largest state bank, *Búnadarbanki*, under the control of Iceland's Progressive Party. In 2004, Iceland's prime minister was a member of the *Independence Party*. Seizing this

[2]Crowdsourcing is a popular term denoting the utilization of knowledge or resources from a vast amount of people through ICT in order to achieve certain added value. The online encyclopedia Wikipedia, for example, uses crowdsourcing for its content. Another example is Facebook's crowdsourcing of facial images by motivating its users to tag faces of their acquaintances.

opportunity, the prime minister "considered it necessary that Landsbanki [the second largest state bank] would land in the hands of persons within at least shouting distance of the Independence Party" (Gylfason, 2012, p. 15). This was accomplished such that the *Búnadarbanki* loaned a significant part of the purchase price for the *Landsbanki* to Russian investors. This loan was never repaid, which led to a "spectacular financial crash in October 2008 when three banks comprising 85 percent of the country's banking system collapsed within a week, and the domestic equity market was virtually wiped out overnight. The rest of the banking system crashed in quick succession" (Gylfason, 2012, p. 3).

After the crash, protests in 2009 forced the government to resign and a new parliament, controlled by a coalition of two left-wing political parties, was elected. This parliament planned and backed the process of drafting a new constitution. The first step was to appoint a national assembly of 1000 citizens, randomly selected via a method that assured "equal representation of men and women of different age groups as well as of different parts of the country." This assembly was then called on to provide a document of elements that they would like to see in the new constitution. This document was produced in October 2010 during a one-day meeting that took place in Reykjavik, whereupon from within the national assembly a group of 25 people were democratically elected to elaborate on the constitution. From the initial 1000 citizens, 523 competed for the 25 seats of the constitutional council. The voter turnout at these elections was 37%, less than half of what Icelandic ballots usually yield (Gylfason, 2012, pp. 12–13).

Throughout the process of drafting the constitution, the public were invited to contribute and discuss. To enable this, a Web forum was opened on which approximately half of the constitutional council's members were interacting with the public. As Magnusson, a member of this council, reports, "at least 4 out of 100 articles in the constitutional draft were directly influenced by the online conversations" (Magnusson, 2013)—a rather low number, which hardly justifies the constitution to be considered crowdsourced. Despite all effort, this constitution was later declared invalid (Gylfason, 2013).

All of the above-described cases utilized simple Web forums. Neither the methodology nor the technology was special in any way. It would be wrong, though, to diminish e-Democracy's potentials based on these examples alone. Though rare, conceptual and technological innovation in e-Democracy exists: one such example is *Liquid Democracy*, which shall be discussed in Section 3.5, and another is Velikanov's vision of *Mass Online Deliberation*

(Velikanov and Prosser, 2017). Rather than asking himself the question of how to attract the masses to participate, Velikanov focuses on the challenge of how to build consensus between mass contributions in such deliberations (once they occur). For this, he proposes a model based on mutual appraisal among the participants, similar to the academic peer-review system.

2.1.4 Open Government Data

The push to technicize the public apparatus was later enhanced by the drive for *open government*. Open government is a doctrine in which government accountability should be assured by government agencies, and allows insight into their internal affairs. In Western societies, this (modern) doctrine dates back to the age of Enlightenment, if not further, i.e., since the emergence of the modern public apparatus.[3] Since this, open government has been the turf of the press, whereby the press can be considered a vital part of the *fourth estate*. In this role, the press has the mission to uncover and publicize the public apparatus' moral misdeeds. In this *watchdog* role, the press has the power to bring down those in power, and in this capacity, the media remains a lucrative business, besides its agenda setting and entertainment functions.

Instead of aiming for a digital *right to know*, the strategy of e-Gov's open government concept aimed for a humble *permission to recycle*: e-Gov's open government is called OGD, or just *open data*, as it is not strictly restricted to the domain of government agencies. In terms of technical requirements, OGD substantially differed from e-Gov. e-Gov was mainly about providing an online channel for access to information and services of government agencies with no specific technical requirements. OGD on the other hand, required that data which are put online should be structured and machine readable so that it could be used (preferably free of charge) by enterprises that could then add value to it. The big push for OGD came soon after the IT industry recovered from the bursting of the dot-com bubble (ca. 1999–2001), i.e., after 2005.

OGD is tightly connected to the efforts of Tim Berners-Lee, the author of the HTTP protocol and the HTML language. In the public discourse,

[3]The emergence and growth of the public apparatus is discussed in Chapter 5. Open government should not be understood as an unconditionally intrinsically positive achievement of the age of Enlightenment. Open government's call for transparency under the pretext of protecting freedom is purely ideological and does not stand on its own without concrete enforcement. This opens opportunities for new agencies to emerge to protect open government, which results in a further growth of the public apparatus.

Berners-Lee is often wrongly hyped as the man behind the Web (or even worse, the Internet as such), and although he did sire it academically, the credits for the complex system of technologies, which give us what we today call the Web, belong jointly to the ecosystem of zealots and volunteers behind an incredible range of technologies.[4] The initial vision of the Web was that of an interconnected network of data in which Web sites (or parts thereof) are connected through hyperlinks. These *resources*, as they are called, are then available on the Web (hosted on Web servers), where they can be fetched, generated, updated, amended, or deleted, within the limits of access rights granted by the Web server.[5] The flagship idea of resources interconnected in a web of knowledge had later been continued by Berners-Lee's *Semantic Web* concept (Berners-Lee et al., 2001), which was about machine-readable semantic annotations of information stored on the Web,[6] and then again by his *Linked Data* (Berners-Lee, 2009) concept, which picks up the ur-WWW idea of interlinking data, in order to make a Web that could be queried by query languages like SPARQL (Berners-Lee, 2009). In this central vision, OGD is the Web, the Semantic Web, and Linked Data, combined: the public authorities ought to publish data (public sector information, PSI), which they collect as part of their provided social function in a clear, preferably semantic structure (e.g., as RDF[7]), which then can be queried and interlinked by SPARQL and the like.

[4]Here we find technologies such as CSS (proposed by Håkon Wium Lie in 1994, later extended by Bert Bos in 1995); the Web browser (Berners-Lee's 1990 *World Wide Web*, Pei-Yuan-Wei's 1991 *ViolaWWW*, Andreessen and Bina's 1993 *Mosaic*, which was then further developed into Microsoft's Internet Explorer); Brendan Eich's 1995 *JavaScript* language; the JPEG image compression format; and a broad range of search engines, from pre-Web search engines for FTP or Gopher (Web's main competitor at that time) such as Emtage's 1990 *Archie* for FTP, Jones' 1993 *Jughead* for Gopher, Foster and Barrie's 1992 *Veronica* (also for Gopher), Gray's 1992 *World Wide Web Wanderer*, the probably first Web bot fueling the *Wandex* Web index, up to Brin and Page's *PageRank* algorithm, which was used to fuel the now dominant Google search engine (to name just a few of the crucial and pioneering technologies that made the Web what it is today).

[5]The actions are denoted by the *methods* (*verbs*) provided by the HTTP protocol. The two most frequently used are GET (fetches/gets a Web resource) and POST (submits data to a Web resource)—almost all interaction on the Web is done through these.

[6]Semantic snippets (structured data) allow for rich presentation of search results in search engines such as Google, where, for example, opening times of shops and organizations, user ratings, or linked advanced information can be displayed in advanced ways. This information is then harvested from the Web by the search engines' bots, i.e., extracted from the Web sites which embed it. As of 2016, schema.org is a well-supported system for encapsulating semantic information in Web sites.

[7]Resource Description Framework.

Making government data available online to the public had already been achieved during the 1980s, when governments were able to publish their data as flat files over FTP. A global demand for online PSI was built from the late 1990s to 2009, pushed by politics, news publishing houses, researchers, etc. (Heimstädt et al., 2014). In the European Union, for example, the 2003 *PSI Directive 2003/98/EC* provided a legal mandate for its member countries to encourage the reuse of public sector data; in 2013, this directive was amended to align with (by the then developed) open data principles. In 2009, this hype reached a turning point, with first governmental OGD portals being released.

OGD was boosted, "blitzkrieg-style" (Peled, 2014, p. 58), by US President Obama's election campaign in the United States and was immediately followed by a strong PR buzz: "[OGD] architects continue to claim that [OGD] mobilized the expertise of the masses, harnessed the hidden desire of agencies to share data, and gave birth to a community of innovators. […] The Obama administration and the media highlighted how [OGD] helped the economy and lowered the cost of governmental operations. Police crime maps and school performance tables attracted millions of visits. Stories appeared about organizations that used [OGD] to build life-saving applications such as one that helps people make informed decisions about heart surgeries" (Peled, 2014, p. 60). The US *data.gov* portal gained prominence as a transparency tool of Obama's presidential campaign, backed by Californian tech entrepreneurs such as Tim O'Reilly (O'Reilly, 2008) who speculated on a new tech boom (cf. Lathrope and Ruma, 2010). This initiative was later continued as the official government's transparency portal (Schulman, 2010).

The roots of the OGD hype are to be found in the 2007 *Sebastopol meeting* (Malamud, 2007), organized by Tim O'Reilly (O'Reilly Media) and Carl Malamud (*public.resource.org*), and supported by the Sunlight Foundation, Google, and Yahoo. The meeting was attended by 30 Internet activists, among them Lawrence Lessig (*Code 2.0*) and Aaron Schwarz.[8] This "Californian" hype soon spread to the whole of the United States and to Britain, which commissioned Berners-Lee to establish and lead the *data.gov.uk* portal.

The crux with OGD is that the published data is generally of little relevance. OGD portals have become dumping yards for government

[8]Schwarz became famous for his pro-piracy stance and activism in the course of anti-SOPA (US Stop Piracy Act), and for aiming to make a large quantity of articles from the JSTOR system publicly accessible. In 2011, he was arrested and convicted, and committed suicide in 2013.

analytics and high-level statistical data with little added value. To give an example, US federal agencies, which, by decree from Obama, had to publish at least three of the high-value sets of statistics or other information in a downloadable format, "went for the low-hanging fruit for things that are already there and not terribly controversial"—the published material contained barely relevant statistics, such as data about child-seat safety, the jail population, or the population count of wild horses and burros (O'Keefe, 2010).

While this kind of data might be an interesting source for students to play with, one cannot truly derive any further value from it. This does not mean, however, that government data cannot be exiting and valuable. The *government data* released in 2010 through the WikiLeaks whistle-blower platform caused an unprecedented amount of information to enrich and shock hundreds of millions of civilians, researchers, and governments around the world (Cammaerts, 2013). News-worthy data do not need to be obtained illegally, though. The freedom-of-information (FOI) legislation in place in systems such as the USA, the UK, or the EU is a great enabler of access to information, including that which public agencies would prefer not to reveal. The British *Parliamentary Expenses Scandal* of 2009 tells the story of the power of this device, as shall be explored further in Section 3.4.

2.1.5 Smart Cities

While e-Gov was occupied with the broad area of the public administration, the desire to technicize the urban space gave birth to a new buzzword: the *smart city*. Like most of the buzzwords used to describe the technization of the public apparatus, smart city is a white rabbit term with no specific meaning. It is used in a broad range of disciplines ranging from urban planning (architecture), politics (citizen participation/e-Participation), computerization and digitalization (remote maintenance of urban infrastructures), and urban billing (systems like Hong Kong's Octopus card or London's Oyster card). But foremost, the smart city buzz is an economy of the public apparatus that fuels markets, by promising progress, while shielding the public apparatus from accusations of stagnation. Market volume estimates for the smart city economy are forecasted to reach $3 trillion by 2025, or $38.9 billion, respectively, to have been spent in 2016 alone (Anthopoulos, 2015).

The smart city narrative unfolds along several dimensions, which do not necessarily involve ICT. Thus, Anthopoulos (2015) outlines six dimensions: *people* (discovering and meeting present and future requirements), *living* (quality of life and social coherency), *environment* (protection, waste and emissions control, and climate change), *governance* (ensuring urban utility and service availability), *economy* (city competitiveness and sustainable growth), and *mobility* (urban transport and traffic management). These dimensions reflect the intrinsic vagueness of the concept and the lack of a clear agenda or definition—there is no clear set of characteristics to recognize a city as a smart city. The smart city is more so a loose bundle of public policy target visions than anything else.

2.2 MYTHS OF E-GOV

In the course of national e-Gov reforms, the promise conveyed by politics and public administration alike was nothing short of a revolution of epic scale. The so reformed administrations were promised to be faster, simpler and more effective, more inclusive, and participative. The drive for e-Gov was fueled over the years, which urged governments worldwide to develop and implement e-Gov policies and artifacts. The push for e-Gov at the turn of the millennium was one of a series of themed business development pursuits carried through corporate storytelling in the context of the technization of the public apparatus. This succeeded the fad around *business process reengineering* (BPR) that emerged at the beginning of the 1990s (Lenk, 2004, p. 59), before the Web became popular enough to conjure up e-Gov—with which BPR partly fused.

Citizen-focused ideas are particularly susceptible to exploitation. Such ideas are used to justify increased use of public resources to fuel the economy and to create new jobs for the public apparatus. It is easy for politics to push for *reforms through technology* and thus generate a PR buzz, which gives birth to stories which leave "no place for social or natural actions that can stop them" (Mosco in: Bekkers and Homburg, 2007, p. 375). This section provides an overview of the corporate narrative for the smart city, based on the research by Ola Söderström, Till Paasche, and Francisco Klauser (Söderström et al., 2014); the myths created via e-Gov policies and PR buzz (research by Victor Bekkers and Vincent Homburg (2007)); and the continued growth of the expenses of public administration, which contradict the promises of e-Gov (Paulin, 2015).

2.2.1 Four Myths of e-Gov

> *MacIntyre has pointed out that myths are neither true or false, but living or dead.*
>
> ***(Bekkers and Homburg, 2007)***

Bekkers and Homburg, in their analysis of e-Gov-fueling public policies, identify four myths—"hymns to progress, utopian visions, unfulfilled or unfulfillable promises." Myths, they argue, are more than falsehoods, but rather:

(1) powerful stories that inspire people to strive for the realization of issues that matter, whatever the cost, and

(2) discourses in which specific aspects are highlighted and revealed at the expense of other aspects that are (deliberately or unintentionally) concealed.

No government, they argue, "can resist the impact of modern ICTs," which invites policy-makers, politicians, bureaucrats, and consultants to "tell stories about the nature of policy problems and how these problems should be tackled." These storytellers then "compose heroic narratives to inflict changes in ways of thinking and doing." The promised innovations, however, "are not necessarily implemented immediately (if at all); nor does the implementation necessarily follow the story lines exemplified in policy documents." The "hopes for immediate implementation and fear of lagging behind," they argue, "make for powerful technomania."

The "purified image of a new and better government" achieved through e-Gov is the first such myth, which promises a digitalized administrative machine "that is responsive, client oriented, and cohesive." This myth announces a new form of technology-empowered government, which "makes life better for citizens and businesses," who will provide electronic services to deliver what people really want. This myth, they note, was a core driver behind e-Gov's *one-stop-shop* idea, in which a single point of access is available to electronic services and information offered by various public authorities (Wimmer, 2002).

To realize the *one-stop-shop*, Bekkers and Homburg argue, would require the coordination of a multitude of heterogeneous back offices within the public administration and "the integration of several information domains, each with its own legal framework, its own information systems, its own data definitions, its own routines and procedures, its expertise and experience, and its own frames of reference." The result of this attempt for progress is thus a "battle of the back offices," which obstructs the development of a sustainable and goal-oriented e-Gov system of systems.

The second myth Bekkers and Homburg identify is the unconditional belief and trust in the use of ICT by the public administration as a driver and core enabler for *technological progress and instrumentality*. The information society "is seen as developing into an open and decentralized society" as part of a "revolution in progress that cannot be missed. The only question is how to respond to it." According to this myth, the public administration "has a moral duty to use the most advanced 'tools' to reinvent government," due to which institutional change takes place. This myth, however, they note, contradicts findings that the introduction of new technologies in the public sector "very often strengthens the existing frames of reference, power relations, and positions within a policy sector."

The third myth is the presumption that the realization of e-Gov artifacts is based on *rational information planning*. Thus, most of the policy documents which Bekkers and Homburg studied focused on high-level goals, rather than on defining clear implementation strategies and realizable technical artifacts. In the course of designing concrete plans for the needed systems, system architects face challenges with consolidating the various requirements among heterogeneous back offices. Such efforts in aligning procedures and functional requirements can fuel existing interorganizational tensions and conflicts. Heralding strategic planning while ignoring the implications of interorganizational interoperability, they argue, has given rise to the myth of rational information planning.

e-Gov policies and strategies aim to deliver to an ideal, empowered, *omnirational* citizen, who "knows his or her preferences, is able to master both bureaucratic and ICT skills, and actively engages in conversation with government agencies." This fourth myth of the *citizen as empowered consumer* of government services is crucial for the legitimacy of e-Gov reform strategies, as without such an imagined citizen, who demands reforms, the e-Gov economy would lose its legitimacy.

2.2.2 The Obligatory Passage Point of the Smart City

The ambiguity of the smart city concept is not its weakness, but rather, its main selling point. The buzz around the term, and the fuzziness of its interpretation, provides a vacuum in which new economies can thrive and authorities emerge. "Smart city" was a major point on the agenda in the European FP7 program for research funding in the domain of ICT, and became even more prominent in the following program, Horizon 2020.

Now it is almost essential for a city to be labeled "smart." Accordingly, there is a "smart" Shanghai (Zhu, 2015); "smart" Moscow, Dubai, and Peterborough (peterboroughtoday.co.uk, 2015); "smart" Vienna;[9] "smart" London (Munford, 2015); and many more. What these cities all have in common are urban infrastructure, public transport, employed and unem-

[9]https://smartcity.wien.at/site/en/.

ployed inhabitants, and their daily struggle for life. With regard to technology, they all use state-of-the-art communication, have their e-Gov presence, might use computerized systems to administer the city illumination and supervise traffic, might deploy sensors to measure air pollution, and so on. But this is all pretty much the state of the art as to what a modern governed urban space implies, this is not where the magic of smart city is to be found.

To understand the drive behind this buzz, Söderström et al. (2014) traced the roots of the smart city story back to IBM's strategies to venture into the vast, yet untapped, market of cities. The rise of the Web during the 1990s and around the turn of the millennium had inflicted huge losses on IBM, leading to the company's move away from hardware design and production to consultancy and software. The new strategy oriented itself away from grounded manufacturing to the *magic* of abstract smartness, which was manifested through its *Smarter Planet* campaign.

The Smarter Planet campaign was IBM's transition into becoming a global player in the public apparatus. Its products are no longer addressing the needs of hard-working entrepreneurs, but rather aiming for the more flexible pastures of urban governance—while the market is easily saturated with respect to selling hardware components, software- and consultancy-based services and products aiming to support the agencies of the public apparatus know no upper limit. Modern buzzwords, such as *big data*[10] (here, IBM's Watson system promises miraculous insights), the *Internet of Things*, the *future Internet*, the *smart city*, or *blockchain*, are no longer about technological advances, but rather about generating as much value as possible from a new hype before it wears off.

This mentality is reminiscent of *The Emperor's New Clothes*, a popular children's tale by Hans Christian Andersen, in which two weavers sell imaginary clothes to the emperor at high prices. They sell these "clothes" claiming that they are invisible to those who are unfit for their positions, stupid, or incompetent. Their miraculous technology, naturally, is a strict trade secret of the weavers, who have managed to position themselves highly in comparison to the competition, who are only capable of producing normal clothes.

To help advertise its smart city solutions, IBM equipped two flagship cities—Singapore and Rio de Janeiro—with software to provide

[10] "Big data is like teenage sex: everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it"—Dan Ariely, 2013, https://www.facebook.com/dan.ariely/posts/904383595868.

for central computerized supervision and steer urban infrastructure. The showcase project here became Rio de Janeiro, where IBM and Cisco set up a futuristic operations center to manage the city's traffic, utilities, and emergency services:

> *Rio de Janeiro's utilities, traffic systems, and emergency services has been managed by a single 'Ops Center,' a huge hub of technologies provided by both IBM and Cisco. With 300 LCD screens spread across 100 rooms, connected via 30,000 meters of fiber optic cable, Ops Center staff monitor live video from 450 cameras and three helicopters, and track the location of 10,000 buses and ambulances via GPS. Other screens output the current weather, and simulations of tomorrow's weather up to 150 miles from the city—and yet more screens display heatmaps of disease outbreaks, and the probability of natural disasters like landslides. There's even a Crisis Room, which links the Ops Center to Rio's mayor and Civil Defense departments via a Cisco telepresence suite.*
>
> ***(Honan, 2012)***

In addition to Singapore and Rio, IBM opened the Smarter Cities Challenge, a program in which cities around the world could compete for three-week pro bono consultancies from IBM to help them transform their city into a "smart" one. "Since 2010 [till 2015], IBM has deployed 800 top experts to help more than 130 cities around the world" (smartercitieschallenge.org, 2016), which gives them massive insight into cities and access to the worries and ambitions, as well as a superior position in subsequent sales activities.

The narrative of the "pre-smart" city as conveyed by IBM's program is that it is an ill, dystopian place with "rising urban populations, ageing infrastructures, and shrinking tax revenues [...], volatile markets, financial deficits," which is "hampered by inadequate systems to serve basic needs, obsolete and broken technologies, litigation costs, benefit frauds, and wasted time. In short, the picture is grim and cities appear close to a fatal breakdown" (Söderström et al., 2014). In this myth of a dystopian reality, the smart city comes as the *fiat lux*, which solves the complex problems of the urban public apparatus by the magic of ICT. The smart city concept thus becomes an *obligatory passage point* (OPP), whereby the latter is "a place (a geographical one or an institution), or a procedure that becomes unavoidable."

Once the smart city buzz reached the status of an OPP, it turned into a self-sustaining economy, in which the value is produced in its own virtual existence. The so created economy will continue until the hype wears off or is replaced by another one.

2.3 A BROKEN PROMISE

Under the pretext to please the *optima-forma* citizen, myriads of information systems were purchased by the public apparatus. Alas, research shows that neither citizens nor public apparatus stakeholders accept e-Gov as planned. Cordella (2007) and Cordella and Iannacci (2010), in part referring to IBM's former head of government services, Todd Ramsey ("No gain without pain: A Survey," 2000), argued that 70%–87% of all e-Gov projects were failures. Studies on OGD revealed a bureaucracy that does not care (Adair et al., 2007; Paulin, 2010b), and studies on the acceptance of systems, such as state-driven electronic identity, reveal acceptance rates that tend toward zero if citizens have alternatives to choose from (Kubicek, 2011; Rissanen, 2010).

e-Gov reforms promised to make the state (aside from the ambiguous "better") more responsive, inclusive, and efficient in terms of handling interactions with citizens. Consequently, if the state was to become more efficient, this should be reflected in some form of externally measurable outcome.

A study attempted to measure the outcome for Slovenia, based on the financial and operational statistics of the Slovenian government, the courts, and the national social insurance agency ZPIZ (Paulin, 2015). Slovenia is a central European country with a very high human development index (equal to Finland as of 2013 (UNDP, 2013)), a member of the EU, NATO, and the OECD. According to e-Gov surveys that measure e-Gov maturity, Slovenia was found consistently among the top in its class. In 2009, it was among the top five in Europe (Capgemini et al., 2009; *The Economist*, 2009); however, by 2012 it had lost its top rank at the European level, but nonetheless remained second at the level of Southern Europe (UN, 2012). After its succession from Yugoslavia in 1991, Slovenian public administration underwent an 8-year transitional period to catch up to Western European standards. Between 2000 and 2003 further reforms took place to adjust the Slovenian administration, judicial, and legal systems to reach the requirements for joining the EU, including a civil servants reform (Pinterič, 2010a). By 2006, Slovenian e-Gov was mature (Pinterič, 2010b). As far as the courts were concerned, a novel e-Justice system (e-Justice refers to the digitalization of processes and workflows in the justice system) was introduced in Slovenia in 2009 with the claim that the "operating costs of courts, as well as all other law enforcement agencies, will reduce significantly. The proceedings will be faster and clearer, the work of law enforcement agencies will become easier, and citizen and businesses involved in the proceeding will get an easy way to access the information" (Bezeljak, 2009; Paulin, 2015).

Taking into consideration that the Slovenian e-Gov reforms were fully developed and complete by 2006, and the justice system was accordingly modernized by 2009, the study concluded that the introduction of e-Gov in Slovenia showed no decreasing effect on the expenses of the state, nor was there evidence of an increase in the efficiency of its judiciary system. On the contrary, in all the observed contexts, the costs increased with regard to the expenditure for human resources, even in the years after recession hit Slovenia in 2008. Until the year of the recession, state expenditures increased at all observed levels, with particularly strong increases between the years 2005 and 2008.

REFERENCES

Adair, K., Nielsen, C., Fuchs, M., Byrne, M., Blanton, T., 2007. File Not Found: 10 Years After E-FOIA, Most Federal Agencies are Delinquent. The National Security Archive, George Washington University.

Albrow, M., 1972. Bürokratie. List, München.

Anthopoulos, L., 2015. Defining smart city architecture for sustainability. In: Proceedings of the 14th IFIP Electronic Government (EGOV) and 7th Electronic Participation (EPart) Conference 2015. Presented at the 14th IFIP Electronic Government and 7th Electronic Participation Conference 2015, IOS Press, Thessaloniki, Greece, pp. 140–147. https://doi.org/10.3233/978-1-61499-570-8-140.

Baum, C., Di Maio, A., 2000. Gartner's Four Phases of e-Government Model. Gartner Group.

Bekkers, V., Homburg, V., 2007. The myths of e-Government: looking beyond the assumptions of a new and better government. Inf. Soc. 23, 373–382. https://doi.org/10.1080/01972240701572913.

Berners-Lee, T., 2009. Linked Data [WWW Document]. DesignIssues. http://www.w3.org/DesignIssues/LinkedData.html. (Accessed 26 December 2011).

Berners-Lee, T., Hendler, J., Lassila, O., 2001. The semantic web. Sci. Am. 284, 34–43.

Bezeljak, T., 2009. Elektronsko poslovanje v sodnih postopkih zaradi insolventnosti [Electronic operation for insolvency proceedings]. In: Z Inteligentnimi Sistemi Do Strateške Prednosti. Presented at the Dnevi Slovenske Informatike. Slovensko društvo informatika, Portorož/Ljubljana.

Cammaerts, B., 2013. Networked resistance: the case of WikiLeaks. J. Comput.-Mediat. Commun. 18, 420–436. https://doi.org/10.1111/jcc4.12024.

Capgemini, Rand Europe, IDC, Sogeti, DTi, 2009. Smarter, Faster, Better eGovernment—8th eGovernment Benchmark Measurement. Capgemini.

Charles, A., 2004. Estonia—The State of the E-State. The Baltic Times.

Cordella, A., 2007. E-government: towards the e-bureaucratic form? J. Inf. Technol. 22, 265–274. https://doi.org/10.1057/palgrave.jit.2000105.

Cordella, A., Iannacci, F., 2010. Information systems in the public sector: the e-Government enactment framework. J. Strateg. Inf. Syst. 19, 52–66. https://doi.org/10.1016/j.jsis.2010.01.001.

Coursey, D., Norris, D.F., 2008. Models of e-government: are they correct? an empirical assessment. Public Adm. Rev. 68, 523–536. https://doi.org/10.1111/j.1540-6210.2008.00888.x.

Gauthier, J., 2008. UNIVAC I—History—U.S. Census Bureau [WWW Document]. census.gov. U.S. Department of Commerce. https://www.census.gov/history/www/innovations/technology/univac_i.html. (Accessed 19 February 2016).

Grönlund, Å., Horan, T., 2005. Introducing e-gov: history, definitions, and issues. Commun. Assoc. Inf. Syst. 15.

Gylfason, T., 2012. From Collapse to Constitution: The Case of Iceland. CESifo.

Gylfason, T., 2013. Democracy on Ice: A Post-Mortem of the Icelandic Constitution. openDemocracy.

Heimstädt, M., Saunderson, F., Heath, T., 2014. Conceptualizing open data ecosystems: a timeline analysis of open data development in the UK. In: Proceedings of the International Conference for E-Democracy and Open Government. Presented at the Conference for E-Democracy and Open Government. Edition Donau-Universität Krems, Krems.

Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design science in information systems research. Manag. Inf. Syst. Q. 28, 6.

Honan, D., 2012. The Automation of Rio: Smart City or Digital Tyranny? Big Think.

Jones, B., 2000. A Report on the Feasibility of Internet Voting. California Internet Voting Task Force, Sacramento, USA.

Kitcat, J., Brown, I., 2008. Observing the English and Scottish 2007 e-elections. Parliam. Aff. 61, 380–395. https://doi.org/10.1093/pa/gsn003.

Kitsing, M., 2011. Online Participation in Estonia: Active Voting, Low Engagement. ACM Press, p. 20. https://doi.org/10.1145/2072069.2072073.

Kubicek, H., 2011. Akzeptanzprobleme sicherer elektronischer Identitäten [Challenges with the acceptance of secure electronic identities]. DuD 35, 43–47. https://doi.org/10.1007/s11623-011-0012-3.

Lathrope, D., Ruma, L. (Eds.), 2010. Open Government: [Collaboration, Transparency, and Participation in Practice]. O'Reilly, Sebastopol, CA.

Layne, K., Lee, J., 2001. Developing fully functional e-government: a four stage model. Gov. Inf. Q. 18, 122–136. https://doi.org/10.1016/S0740-624X(01)00066-1.

Lenk, K., 2004. Verwaltungsinformatik als Modernisierungschance: Strategien—Modelle—Erfahrungen; Aufsätze 1988–2003. Sigma, Berlin.

Lippert, S.K., Ojumu, E.B., 2008. Thinking outside of the ballot box: examining public trust in e-voting technology. JOEUC 20, 57–80. https://doi.org/10.4018/joeuc.2008070104.

Magnusson, F., 2013. Crowdsourcing Icelandic Constitution—A Myth or Reality? Available at: https://democracyoneday.com/2013/03/11/crowdsourcing-icelandic-constitution-a-myth-or-reality/. (Accessed 26 August 2018).

Malamud, C., 2007. Open Government Working Group Memorandum [WWW Document]. https://public.resource.org/open_government_meeting.html.

Mikaelsson, R., Wihlborg, E., 2011. Challenges to local e-Democracy. In: Proceedings of the International Conference for E-Democracy and Open Government. Presented at the CeDEM11, pp. 83–94. Krems.

Miran, N., 2011. Gradnja v lastni režiji [Do-it-yourself Construction] [WWW Document]. Predlagam.Vladi.si. http://predlagam.vladi.si/webroot/idea/view/1565. (Accessed 30 June 2019).

Morris, H., 2012. Crowdsourcing Iceland's Constitution. International Herald Tribune.

Munford, M., 2015. London Leads the Way in the Global Growth of "Smart Cities." The Telegraph.

No gain without pain: A Survey, 2000. The Economist.

O'Keefe, E., 2010. Data Released Under Obama Order Criticized. The Washington Post.

O'Reilly, T., 2008. Why I Support Barack Obama. O'Reilly Radar.

O'Reilly, T., 2010. Government as a platform. In: Lathrop, D., Ruma, L. (Eds.), Open Government—Collaboration, Transparency, and Participation in Practice. O'Reilly, Sebastopol, CA, pp. 11–39.

Oravec, J.A., 2005. Preventing e-voting hazards: the role of information professionals in securing the promise of electronic democracy. J. Organ. End User Comput. 17, i–iv.
Paulin, A., 2010a. Župa—grassroots e-democracy revolution on the web. In: Proceedings of the 4th International Conference on E-Democracy, books@ocg.at. Presented at the EDem2010. Österreichische Computer Gesellschaft, Krems, pp. 113–123.
Paulin, A., 2010b. Slovenia 404—on the e-readiness of modern public administration. In: Proceedings of the International Conference on Information Society and Information Technologies. Faculty of Information Studies, Dolenjske Toplice.
Paulin, A., 2015. Twenty years after the hype: is e-government doomed? Findings from Slovenia. Int. J. Public Adm. Digit. Age 2, 1–21. https://doi.org/10.4018/ijpada.2015040101.
Paulin, A., Welzer, T., 2013. A universal system for fair non-repudiable certified e-mail without a trusted third party. Comput. Secur. 32, 207–218. https://doi.org/10.1016/j.cose.2012.11.006.
Peled, A., 2014. Traversing Digital Babel: Information, e-Government, and Exchange. Information Policy Series, The MIT Press, Cambridge, MA.
Peterboroughtoday.co.uk, 2015. Peterborough Beats Moscow to Smart City of the Year title. Peterborough Telegraph.
Pinterič, U., 2010a. Slovenian local administration reform 1993–2010. Anal. J. 3 (1), 56–64.
Pinterič, U., 2010b. Development of e-government services for citizens in Slovenia. East. Eur. Econ. 48, 88–98. https://doi.org/10.2753/EEE0012-8775480305.
Reddick, C.G., Turner, M., 2012. Channel choice and public service delivery in Canada: comparing e-government to traditional service delivery. Gov. Inf. Q. 29, 1–11. https://doi.org/10.1016/j.giq.2011.03.005.
Rissanen, T., 2010. Electronic identity in Finland: ID cards vs. bank IDs. Identity Inf. Soc. 3, 175–194. https://doi.org/10.1007/s12394-010-0049-8.
Schulman, R., 2010. Government transparency and the Obama ERA. LPB 2, 2.
smartercitieschallenge.org, 2016. Smarter Cities: The Challenge [WWW Document]. IBM. https://smartercitieschallenge.org/about (Accessed 21 February 2016).
Söderström, O., Paasche, T., Klauser, F., 2014. Smart cities as corporate storytelling. City 18, 307–320. https://doi.org/10.1080/13604813.2014.906716.
Stokes, J., 2007. 1,000 Pages of Bad News: Ohio E-Voting Report Released. Ars Technica.
The Economist, 2009. E-Readiness Rankings 2009. The Economist Group.
UN, 2012. United Nations E-Government Survey 2012 (No. ST/ESA/PAD/SER.E/150). United Nations, New York.
UNDP, 2013. 2013 Human Development Report. United Nations.
Veit, D., Huntgeburth, J., 2014. Foundations of Digital Government—Leading and Managing in the Digital Era. Springer-Verlag.
Velikanov, C., Prosser, A., 2017. Mass online deliberation within participatory policy-making. In: Paulin, A., Anthopoulos, L., Reddick, C.G. (Eds.), Beyond Bureaucracy. Public Administration and Information Technology. Springer.
Wimmer, M.A., 2002. A European perspective towards online one-stop government: the eGOV project. Electron. Commer. Res. Appl. 1, 92–103. https://doi.org/10.1016/S1567-4223(02)00008-X.
Zhu, S., 2015. Shanghai Deal to Turn Into Smart City. Shanghai United Media Group. ShanghaiDaily.com.
Zinner Henriksen, H., 2012. In the beginning was the CCR. In: Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and IFIP EPart 2012, Schriftenreihe Informatik. Presented at the IFIP EGOV 2012. Trauner, Kristiansand, pp. 13–20.

CHAPTER 3

Controlling Citizens or Controlling the State?

Contents

Introducing technology into the many functions of the public apparatus awoke new hope to streamline government agencies and democratic processes, harness governments and public institutions, and finally subject them all to the full control of the sovereign (in theory, in a democracy the sovereign is the community of citizens as such). Such hopes are justified as, after all, *information and communication* technology (ICT) has introduced a powerful solution to avoid a nearing *postgrowth society*[1] of the 20th century: The Internet, engineered in the 1970s, and its later killer applications that came as the Web's bundle of technologies (engineered throughout the 1990s and the first decade of the 21st century) created the *cyberspace* as we know it today. The cyberspace has introduced a novel dimension for human interaction, in which production, trade, invention, creativity, and communication can take place in ways that have never before been possible in the entire history of the human race.

Alas, the hopes to subject the public apparatus to the control of the sovereign did not materialize. As cyberspace matured, the public apparatus was quick to spread into cyberspace in various forms, for example, global

[1]The term is used by social scientists to denote the end of the era of growth that we have become accustomed to throughout the past few decades. From the point of view of production, this era has been already reached. Characteristic to the *postgrowth society* are redistribution battles, as resources become more and more scarce.

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00003-0

espionage by the US National Security Agency (NSA) disclosed by the 2013 Snowden leaks, the 2010 sabotage of the Iranian nuclear program by the Stuxnet virus, the 2007 cyberattacks on Estonia, the 2012–16 SWIFT sanctions on Iran, the capital controls in Greece from 2015, the European data retention legislation under the pretext of terrorism control, or the 2016 Apple vs. FBI showdown (Cringely, 2016). These all tell stories of an increasingly threatening and aggressive public apparatus, and a significant reduction of democratic control.

3.1 THE TRANSPARENT SUBJECT

The invasion of cyberspace by the public apparatus reflects a dangerous drift into a *postpolitical* era. Technology is utilized to its full potential to empower the public apparatus and to make its subjects increasingly transparent. Aside from using technology for aggression (espionage, sabotage, and warfare) and reduction of civil liberties (biometric tracking of movement, capital controls, etc.), technology is heavily deployed by the public apparatus to structure and control its subjects in the finest manners of George Orwell's *1984* (Orwell, 1949).

In modern Slovenia, citizens have central access to many governmental repositories. Using an e-ID, citizens can log into their personalized portal and browse through some of the data stored about themselves: when they were born, their place of permanent residence, their address for receiving mail, marriage status, tax number, their unique citizen identifier, which ID documents have they been issued and until when are they valid, which cars do they own, what is the mileage on these cars, the cars' identification numbers, license plates, and registration certificates, etc., what real estate do they own and what is its estimated worth for tax purposes, etc. This is, however, only a small and rather shallow selection of the data the Slovenian state has about any given citizen. The state also knows where one is employed and under which conditions, how much interest they got on deposits in other countries, where, when, and for which reason one has been convicted by a court, which bank accounts one owns, and so on.

The collection of data about citizens is legitimized by law and necessary for digitalized administrative processes and cross-sector integration of backend systems. To this end, collecting and exchanging data by and among governmental institutions has positively transformed the experience of citizens in dealings with the state. Bovens and Zouridis (2002, p. 174) remind us how it was in the former times:

> *Bureaucrats are well known to be small-minded pencil pushers who can reject or approve an application for no better reason than the fact that your existence has somehow annoyed them. This was the specter that haunted Weber, Hayek, and Popper: Large numbers of faceless officials whose freies Ermessen (discretionary power) could cause an open society to be smothered in the bud.*

Our world has changed, obviously, from the times of Weber, Hayek, and Popper. Much of the bureaucratic discretionary power today is confined to back-office cubicles and has undergone the transition from a purely *street-level bureaucracy* to a *screen-level bureaucracy*, or even a *system-level bureaucracy*. But what do these terms mean?

Street-level bureaucrats are "public employees who interact directly with individual citizens and have substantial discretion in allocating facilities and imposing sanctions" (Bovens and Zouridis, 2002). As of today, this includes, for example, street police, teachers in public schools, medical staff in public health services, construction authorities, all of whom make decisions on the level of individuals based on their professional observations. This discretionary power of street-level bureaucrats is an ever-present potential source of injustice and corruption within the system, which has justified the rise of legal principles such as the *principle of legality*, which limits the actions of officials to what is explicitly allowed.

Screen-level bureaucracies structure and routinize the decision-making process through digitalization. Information processing systems allow, and mandate, that the information required for decision making is captured and stored in a digital structure for communication and processing. This ensures that decisions are made removed from the subject concerned and thus in an anonymized way. Screen-level bureaucrats are presented with the data via computer applications, from which they make a decision. Recommender systems can then be applied to make automated suggestions for decisions based on the information available in the system.

System-level bureaucracy goes a step further. Here, advanced information systems can function without explicit human involvement from the side of the bureaucracy. Information systems can be interconnected to such an extent that information is automatically collated from various sources, and applications from citizens can be handled instantly—e.g., approved, rejected, or set aside for manual inspection.

Both screen- and system-level bureaucracy rely on heavy data processing, for which they require the citizen to be as transparent as possible. In Slovenia, one no longer needs to *hand in* a tax return, as the state will already know everything in regard to the citizen's income from work, capital owned in the form of real estate or shares, and so on. This might sound practical (and is), but it is equally a system which is grossly imbalanced: If the state has a technological lever so as to "pull" the taxes from its citizens, then where is the equivalent lever for citizens to steer the state?

Increased technization empowers the public apparatus, though at the same time the ability to democratically control the public apparatus is reduced. This drift away from a state in which public apparatus action can be controlled is called *postpolitics*. This drift bears huge risk, as discussed in the following sections.

3.2 E-GOV'S POLITICS OF UNSUSTAINABILITY

Sociologists have criticized that society has reached a state in which the structural status quo of the public apparatus is no longer sustainable, though in politics one aims to preserve this unsustainable status quo; Blühdorn (2014, 2007) calls this state the *politics of unsustainability*. The same critique applies to the situation in which the technization of the public apparatus is stuck.

The manner in which the computerization and digitalization of the public apparatus has progressed has resulted in unsustainable monolithic systems. Future generations will lose political and legislative control over these systems, as traditional politics and law are not capable of governing the code of these systems. Such depoliticized systems, which have broadly been deployed throughout the last decades in many layers of the public apparatus, are not only a crucial contributor to the fortification of a *postpolitical society* in which popular sovereignty has shrunk to the level of symbolic rituals (Blühdorn, 2007), but also lead to a new era of supremacy of *too-big-to-fail* technological infrastructures. This supremacy of those who control these technical systems may well place society on a trajectory toward a new form of feudalism.

How can such dawning feudalization be prevented? New bureaus and new organizational measures would only further the continuity of the *politics of unsustainability*. It would be naive to search for salvation by, for example, intensifying the involvement of supervising agencies or similar; organizational measures often turn out to be mere paper tigers.

To overcome unsustainability, the challenge primarily becomes a technological one: Technology which is used to build information systems to govern society is ICT. As the name implies, it addresses situations of communication or information processing. Even though both *communication* and *information* may well play important roles in societal governance, ICT does not fully address the entire spectrum of requirements that constitute governance. Governance is foremost about power, collective decision-making, and the thus conducted control of public domain resources and action.

Awareness must be prioritized for the implications of the ongoing politics of unsustainability in the domain of technical systems for digital governance. Such discussion needs to be cultivated as a trans-disciplinary debate, which is necessary in order to build a strong foundation for a sustainable future in democratic organization. From the perspective of democratic control, modern technical systems for governance have two dangerous implications: First, tech-savvy organizations that control such systems become monopolists over the social function which their system provides, which allows them to brutally discriminate potential competitors from providing alternative solutions; second, the expert knowledge required to maintain and change such systems is so complex that only a handful of engineers would know how these systems work in detail.

3.3 DAWN OF TECHNO-FEUDALISM

Before the digital era, the work of bureaus was easily controlled by law, morality, markets, or technical architecture—by changing law, for example, one could change how a bureau operates. Bureaus' operational capital, infrastructure, and knowledge are tangible and comparably easy to control, as long as it was comprised of things like real estate, railway tracks, mechanical machinery, registries, or physical files. In such a context, bureaus were controlled by means of a public-law legal system, which could be subjected to democratic principles.

The digital era has brought change to the bureaus' means and tools. The transition from street-level bureaucracy to system-level bureaucracy has introduced a new type of asset in the portfolio of bureaus, namely, large-scale information systems which virtualize and automate the bureaus' functions. The ownership and control over such systems have allowed bureaus to gain the upper hand in relation to legislators, as the functioning of society has become systematically dependent on these *too-big-to-fail* bureaus. The resulting systems thus become sinecures over which future legislators will have no control.

The monopoly of control for the terms and conditions under which the bureaus' technical systems are used bears danger to lead to a neofeudal order, which excludes political competition and imprisons society within a functionally frozen societal system. The evolution toward digital feudalism has been previously discussed in the context of Internet governance with regard to digital communications hardware (Meinrath et al., 2010), but is a novel notion in the context of technology for the governance of the public apparatus. This evolution impacts the legitimacy and regulative abilities of the democratic order on the one hand, and stifles markets and innovation on the other.

The modern approach to building technical systems which serve the needs of governmental institutions is to build software with specific functionality, e.g., portals to serve information; back-end systems to store, manage, and exchange taxation data; or systems to administer data and process it as relevant to the other manifold stakeholders of the public apparatus, such as health-care providers and political organizations. As a result, each of these systems has been carefully handcrafted by system developers and sold to the state with warranty and a service agreement. The crux of such bespoke artifacts, however, is that they fit only to foreseen situations. Changes in law, organizational priorities, or the context in which a bureau operates easily render such artifacts void.

Such systems become publicly funded sinecures, which increase the might of particular agencies and institutions. These in turn grow in strength and independence from law and politics, leading to a shift of societal power away from lawmakers and the public at large, toward feudal enterprises with monopolies over systems such as public registries, accountancy systems, geospatial and cadastral databases, and so on.

3.4 FREEDOM OF INFORMATION VS. THE TECHNICIZED PUBLIC APPARATUS: NO DAVID VS. GOLIATH

In light of the increased technization and *depolitization* of the public apparatus, commitments were made to civil liberties, such as extensive freedom-of-information (FOI) concessions. Section 2.1.4 on *open government data* (OGD) already touched upon Europe's public-sector information directive, based on which many countries enacted modern FOI legislation. FOI is a framework that consists of the *right to request* public information unless righteously restricted (it is not really a *freedom* as the name suggest, but a *claim-right*—cf. Section 6.2), and the national *information commissioner* (IC), a bureau set up to act as an inspectorate and first-instance body in FOI-related matters. FOI is an especially profitable tool for media journalists in gaining access to newsworthy documents which government agencies might be keen to hush up and hide from the public.

FOI is thus the opposite of OGD. While OGD is (generally) structured, open, voluntarily provided by state agencies, and often worthless, FOI comes in the form of photocopies, often heavily censored and redacted, headline-tickling material, and more often than not involves lengthy legal battles to obtain. Obtaining documentation under FOI requires skill and endurance, and, ultimately, one must know what they are looking for—as such, successfully fought FOI battles deserve respect. One such successful FOI battle triggered the *UK Parliamentary Expenses Scandal* in 2009.

In the United Kingdom, members of parliament could claim refunding for expenses, including the cost of accommodation, which they incurred by the performance of their duties, up to a certain allowance. When in 2005 UK enacted its FOI act, journalists Jon Ungoed-Thomas and Heather Brooke independently requested access to information on these expenses for all of the 646 members of parliament. The requests were refused with the explanation that it would be too costly to provide this information. Brooke then separately requested information on the travel expenses of members of parliament (MPs), names and salaries of the staff paid by the MPs, and information on second homes—but all of these requests were also denied. In 2006, she appealed to the IC and thus started a legal and political battle for the requested information, which culminated in 2008 with the release of some incomplete data. By 2009, a full dataset had leaked, which the press purchased for £110,000 (Tryhorn, 2009), thus the embarrassing and partly criminal behavior of the MPs was revealed. The scandal led to the imprisonment of eight MPs for expenses fraud, entertained the British public, yet caused no significant harm in the following elections (Vivyan et al., 2012).

Despite the entertainment value of such public FOI cases, one must acknowledge the complex challenge at stake in understanding what *data* actually means in the context of FOI.

We set out to explore the answer to this challenge by requesting a copy of the database of the Slovenian government's central accounting and human resources management system MFERAC. The MFERAC system was ordered by the Slovenian government in 1996 and underwent renovation during 2008–2009 (Lenarčič, 2009). The system processes and stores data on most of the financial transactions within the Slovenian public sector and, among others, includes information about all public-sector remunerations, the country's social security transfers, paid subsidies, and payments for work commissioned. The MFERAC database is thus *the* most detailed source of information on how Slovenia uses available funds, and who benefits from these transactions. It goes without saying that the thus requested database contains very interesting information for assessing the scale and extent of Slovenia's public apparatus.

Our initial request was first rejected by the Ministry of Finance under the pretext that releasing this information would jeopardize Slovenia's fiscal stability and reveal numerous business secrets and that the information requested contains massive amounts of personal data (RS-MF: Ministrstvo za Finance Republike Slovenije, 2010). Following an appeal to Slovenia's IC, the appeal was dismissed, as the IC interpreted the request to mean a collection of tables exported from the database, which in such form the Ministry neither possessed, nor was obliged to produce (RS-IP: Informacijski Pooblaščenec, 2010). This decision was later successfully contested before court (RS-AC, 2011), which returned the issue to the IC for reconsideration.

The issue was then a matter of two questions: first, what was meant by *data*; and, second, which kind of data could be disclosed to the public? The issue of disclosure had already been resolved in numerous cases across the world,[2] but besides this, Slovenian law stands clear on the issue that *any* data which is not explicitly exempt from disclosure must be made available to the public. Furthermore, disclosure must be granted outright if the requested data is about the use of public funds (which public-sector salaries are). Thus, the proceedings focused primarily on the outstanding technical issues. In its second ruling, the IC decided (RS-IP: Informacijski Pooblaščenec, 2012) that the requested data was indeed *data* and that, in principle, this data could lawfully be disclosed. However, it opined that the requested data contained sensitive private data that must be concealed prior to disclosure. They then analyzed how such concealment could be achieved and found that "data could be exported only if filters [which would conceal nonpublic data] were created before exporting the data, as concealing the data during [the process of] exporting the MFERAC database is not possible" (RS-IP: Informacijski Pooblaščenec, 2012, own translation). What followed was that the Ministry declared itself incapable of concealing the data, which pretty much closed the case.

This case revealed several interesting insights, which confirm the challenges of the digital era as discussed throughout this chapter.

First, there was the question of *what* data had been requested or, more specifically, what in the requested data was *government data*? This question

[2]In the UK, for example, EA/2007/0060, Scottish Information Commissioner 033/2005 and 086/2006; Ireland: Information Commissioner case 99168; European Union: 3643/2005/(GK)WP and ECR I-4989.

is not trivial at all, as it was not a paper-based tangible document that was requested, but rather a complex, multilayered piece of information (the database) that is stored and distributed (i.e., not in one part, but in several parts) throughout a multitude of modules and subsystems of the MFERAC system (this issue is further explored in Section 4.3). The question easily becomes a philosophical one: Is a distributed database a single database (one *document*) or a combination of many separate parts of it (many *documents*)? This confusion was enhanced by the expert witness' ambiguity, whether or not the exported database file—given that it requires dedicated programs to properly consume it—could at all be considered a proper *document* at all (RS-IP: Informacijski Pooblaščenec, 2012b). (The term *document* in the sense of FOI does not refer to a tangible document, but rather to any kind of information no matter what form it comes in.)

Second, the case revealed significant ambiguities on the side of the legal staff (the IC's employees, the courts) who were not comfortable with the technological domain of the matter at stake. This confusion went so far that in the first round the IC misunderstood that the request was for a *photocopy* of the database, rather than a *copy* (i.e., duplicate) of the electronic database; a further confusion was a lack of knowledge in the differentiation between *information system* and *database* on the side of the IC (RS-AC, 2011). This confusion exposes the rift between law and technology, which is explored further in Chapter 4.

Third, and most importantly, the matter demonstrated an inherent reluctance of the MFERAC system to be subjected to law and reflected the techno-feudalistic characteristic of a sinecure to be. The internal architecture and code of MFERAC are de facto out of reach of the legal system, simply for the reason that the expert knowledge and know-how about the system's internal structure are kept locked away by the controlling bureau. The MFERAC system is *the* central system of all affairs related to financial transactions within the public apparatus of the state, with which other public domain bureaus are obliged to interface. Thus, whoever is in control of such a system is de facto controlling the entire state.

3.5 APROPOS: THE PIRATES & CO.

In the beginning of the 21st century, tech-savvy politicians were immersed in the idea of giving the party base more influence in the political policy-forming processes. One of the ideas was to transform the political party into a proxy system that would give voters direct access to political power, whereby the party's candidates would restrain themselves from clear political visions, and instead would act as proxies for opinions and decisions which party supporters (voters or the party base as such) would form direct-democratically by means of ICT, typically through web forums.

The idea to use technology this way to include voters more actively in democratic policy-making was new. It was viable technically, as the Web had become ubiquitously available. It was certainly worth a try to get into parliament or city council by this method. Early proponents of such *proxy parties* were described by Ovid P. Boyd (2008). The studied parties *Knivsta.nu, Demoex, Aktiv Demokrati,* and *Direktdemokraterna* had all evolved from independent groups of citizens. *Knivsta.nu* was formed from an activist group, which succeeded in separating Knivsta (a small town near Stockholm) from another municipality about whom the Knivstanese were not particularly keen. *Demoex* and *Aktiv Demokrati* had emerged from ideas of high-school students and university students, respectively, with the ambition to form genuine proxy parties. While *Aktiv Demokrati* failed to be elected, *Demoex* won one seat in the years 2002, 2006, and 2010, making it the first proxy party ever to win seats in elections (Boyd, 2008, p. 3), before merging with *Direktdemokraterna* and finally dying out in 2014 (Norbäck, 2014). *Direktdemokraterna* was set up to develop an e-participation system to support decision making as in proxy parties, aiming to test it at student elections; however, whether or not this was achieved is not documented. Participation in the system provided by *Demoex* was considerably low, Boyd notes, "possibly due to the unlikelihood of the party's one representative casting a deciding vote."

Proxy parties are an interesting approach toward true representation of subjects in democratic decision making, as they really put the ideals of representative democracy to the test. However, the level of participation generally fails to reach significance. Most experiments of this kind have failed within months of existence, as in the cases of the British *Your Party* or New Zealand's *Direct Democracy Party*, and those that have survived longer than that fail to reach a mandate due to weak public interest, such as the Australian *Senator On-Line*, which yielded 0.06% of the votes in the parliamentary elections of 2007, or *Aktiv Demokrati*, which achieved a meager 81 votes in the Swedish national elections of 2006 (Boyd, 2008).

Proxy parties are no remedy to the public's stubborn disinterest in daily politics. This does not surprise: proxy parties do not offer a strong leader, a core ideology to follow, or an "important" cause to support. The underlying decision-making model of proxy parties is based on the rather idealistic vision that everyone should be granted equal rights to directly express their opinions and preferences on every single matter. But this is not how society functions. The model of democratic representation of the populace before a democratic body is a myth which tells the story that each voter's opinion is to be represented, while in fact, it is only a model that aims to ground the legitimacy of the democratic body in popular will. It could work easily the same way if its legitimacy was grounded in appointment by God or blue blood.

To understand the dynamics of voter behavior, and other trust and position building processes in society, one finds an explanation in Paul Lazarsfeld and Elihu Katz' *two-step flow* theory (Katz, 1957): Individuals tend to be influenced by their peers, whom they trust and interact with. Lazarsfeld and Katz' theory finds application in media studies, where it states that people tend to group around opinion leaders in the process of disseminating, digesting, and interpreting information streamed through mass media. This theory was formulated in the 1940s, but has since been refuted many times, as it fails to stand in the modern context of information streaming through media. The principle itself, however, remains of value, that is, that individuals tend to follow opinion leaders in their public activities and will go to rallies because their friends do so. Individuals will vote for one party and never for another, because their peers do the same, or will abstain from elections altogether, as nobody they know takes part.

Around the same time when proxy parties rose and fell, another political party was founded in Sweden, which has played a more important role in the evolution of digital-era parties: the *Piratpartiet*, the first *Pirate Party*. The Swedish Pirates established themselves in 2006 under the leadership of Rickard Falkvinge,[3] a former affiliate of the Swedish center-right *Moderate Party*. The party pioneered in advocating for reconsiderations of copyright laws and the right to share digital content following Hollywood's *war on movie piracy* (cf. Hennig-Thurau et al., 2007). They rose to national prominence after the crackdown on the globally popular Sweden-based file-sharing hub *ThePirateBay* in the spring of the same year. In the following parliamentary elections in autumn, the party failed to enter parliament, but did so three years later, after a strong sympathy push due to the conviction of the operators of *ThePirateBay* (Zolleis et al., 2010, p. 9).

Following the example of the Swedish Pirates, an allegedly independent pirate party in Germany was established with the same agenda, which at the beginning was scraping a miserable existence. In 2009, the German Pirates succeeded in positioning themselves in the German political scene

[3]Born as Dick Greger Augustsson. *Falkvinge* means falcon wing.

by opposing government plans to censor the Internet under the pretext of fighting child pornography (Zolleis et al., 2010).

Unlike established parties, the pirates rely on the party base for making policy decisions and program guidelines. This, Zolleis et al. (2010) argue, is due to two reasons: First, they do not have a strong party network of auxiliary organizations at their disposal, which could be utilized to define and communicate the party's priorities; and, second, they do not need such a framework, as their target group prefers direct interaction via the Internet. While it can be debated whether or not the German Pirates, with their fresh organizational approach, are just a flash in the pan (Voss, 2013; Zolleis et al., 2010, pp. 31–32), it is their interparty-communication approach that is of interest, and shall be explored in the following subsections.

3.5.1 Liquid Democracy

As a vehicle for collective decision making of the party basis, the German Pirates favored the concept of *Liquid Democracy* (LD) ever since (Jabbusch, 2011, p. 31). LD is a weighted way of making collective decisions, which does not depend on electing representatives. Instead, each member of a society can delegate its power to another member, and withdraw it again at any time (Paulin, 2014). The principle is simple: Let us assume a society of six members—Ann, Bob, Carl, Dan, Eve, and Franck. Let us further assume that each member of the society has an equal share in making a common decision; hence, each has one vote of equal value. Ann has delegated her power to Bob, Bob and Carl to Dan, and Dan to Eve; Franck has not delegated his vote to anyone. Given these delegations, the distribution of power in the society would be as illustrated in Fig. 3.1: Eve would hold 5/6 votes

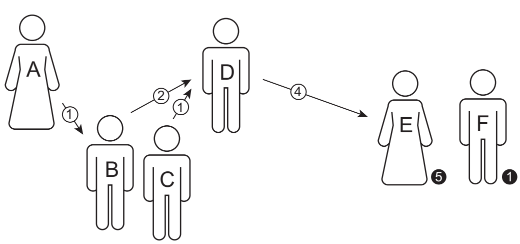

Fig. 3.1 ***Liquid delegation of power.***
A delegated her single vote to B; B and C delegated their votes to D; D, having received two delegated votes from B (including that of A) and one of C, delegates these three plus his own (hence, four) votes to E, who thus holds in sum five votes. F has not delegated his vote to anybody and hence holds his power of one vote.

(hers + Dan's + the delegations Dan received from Bob and Carl + the delegation Bob received from Ann), and Franck would hold 1/6 of all votes.

The magic of LD is that the count of power is only conducted when a collective decision is to be made. A delegated vote is not lost, but the person who delegated it is not burdened with active participation unless they so desire. That is, a delegation can be revoked at any time, which gives the network of delegated trust in LD its characteristic *liquidity*. Thus, in the above example, Dan could revoke his delegation to Eve, which would make him instantly the most powerful person in the society, holding 4/6 of the votes.

LD's base principle is so simple that it is impossible to trace who came up with this idea first—LD may well have developed in many different places independently. Due to its reliance on ad hoc calculation of power relations, the liquidity principle can only be realized through the power of ICT, which provides the essential underlying infrastructure. The first realized instantiation of an LD system is Paulin's Župa (Paulin, 2010), which applied LD to the *Student Union of the Faculty of Information Studies (ŠOFIŠ) in Novo mesto* for executive empowerment. Župa was followed by LiquidFeedback (LQFB), which Behrens, Kistner, Nitsche, and Swierczek developed for the German Pirates (Swierczek, 2014).

By 2016, six different LD instantiations were known, and two active real-world organizations claimed to be using LD: the German *Pirate Party*, and the Canada-based *Industrial Workers of the World* (Oosterveld et al., 2015, p. 47). Besides *Župa* (2009/10) and *LQFB* (2009/10), the other systems were Reinhard Hainisch and David Madl's *Civicracy* (2012) (Hainisch and Paulin, 2016); the Australian Pirates' *Polly* (being developed since 2012) (Downing and Molloy, n.d.); the Russian *democratia2.ru* (2011) by Leonid Volkov and Fyodor Krashenikkov, which instantiates their specific flavor of LD "*cloud democracy*" (cf. Velikanov, 2013); and the 2012 Google Votes experiment (Hardt and Lopes, 2015), which allowed Google employees to make choices about things such as which food their canteen would serve.

Interest in LD gained momentum in the digital government research community soon after the first instantiations appeared. The technical sciences contributed schemes to support LD systems with cryptographically enhanced security features to enable secure and privacy-preserving delegation of power (Bitsch Link et al., 2014; Zwattendorfer et al., 2013); philosophers brought up the idea of a global parliament for world government using LD as an enabler (van Hulten, 2014), and pro and contra discussions emerged whether or not LD is too complex and hence inferior to classical methods of direct democracy (McCarthy, 2013; Nijeboer, 2013). Blum and

Zuber (2016), finally, argued that LD is far superior in terms of making democratic decisions when compared to other models, such as direct or indirect democracy.

Sebastian Jabbusch's 2011 graduate thesis (Jabbusch, 2011), in which he describes the story of the German Pirates, provides a valuable exploration of early ideas related to the LD principle (based on a 2010 article by James Green-Armytage (2010)). Jabbusch, himself a former high-ranked party member of the German Pirates, sees the Internet as an opportunity to get rid of "inefficient and costly organizations like parties and parliaments" and sees LD as an enabler to exchange or completely remove representative democracy (Jabbusch, 2011, pp. 8–9). Through LD, he argues, the people would assume all legislative roles of parliament—committee debates, amendments, formation of opinions, and resolutions regarding even complex wordings of laws whereby citizens would have the right to propose new laws at any time (Jabbusch, 2011, p. 35). He further envisions that individuals could delegate their voting power temporarily to organizations (such as political parties, NGOs, and associations) or to individuals (politicians, experts, friends), or, optionally, a citizen's vote could be delegated only for particular topics or areas of political debate (Jabbusch, 2011, p. 35).

Regarding the history of LD, here is what Jabbusch (2011) found:

In 1912, the *New York Times* reports of William S. O'Ren, who demanded *interactive representation*, whereby each elected politician's (the so-called proxy's) influence would be weighted with respect to the number of votes received. His idea was picked up more than half a century later in 1967 by the mathematician Gordon Tullock, who in passing suggested that voters could "by wire" choose their representative or vote themselves (in parliament) while the debate was broadcast on TV. In 1969, James C. Miller argued that everybody should have the possibility to vote on any question themselves, or appoint a representative. This idea was welcomed by Martin Shubik in 1970, who calls it an "instant referendum," but was concerned that this fast-paced decision-making might reduce the time available for a full public debate.

Jabbusch notes that further occurrences of LD-related ideas can be found in the ideas developed by "sayke," an anonymous user of the Web, according to whom "liquid democracy can be thought of as a function that takes a question as an argument, and returns a list of answers sorted by group preference [… or] as a voting system that migrates along the line between direct and representative democracy" ("sayke" in: Jabbusch, 2011, p. 31, own translation). Sayke's idea was developed further through a wiki until 2003, resulting in the concept that a decentralized information system should enable citizens to participate in political decision-making, thus making parliaments obsolete. Each citizen should have one vote, and the system would provide the citizen with every proposal on each matter at stake. If the citizen did not want to do their own research on a particular matter, they could subscribe to the opinions of their friends instead. The system would further provide that decisions could be made automatically by the system under certain circumstances. The idea was further developed by the anonymous user "Kragg," who dropped the subscription to friends' decisions and instead proposed that votes could be delegated transitively—i.e., received delegations could be delegated further, which is a crucial characteristic of LD.

However, when dealing with the "history" of LD/proxy voting, one must be aware that LD-style collective decision making is not a vision that has emerged from a long-standing incremental academic debate. On the contrary, it is a surprisingly natural way of thinking, which by means of ICT can finally be brought to life.

The crux of LD, however, is that its business model is yet to be found. In the case of Župa, LD was introduced top-down (the organization was set up from scratch under the supervision of Župa's creator), but the organization transformed away from LD even before Župa could be tested in a real environment.[4] A similar fate struck Hainisch and Madl's system Civicracy, which failed to reach the phase of a real-world experiment (Hainisch and Paulin, 2016). When Hainisch and Madl tried to approach an existing student council to use Civicracy in order to widen the participation of students in student politics and increase transparency and legitimacy, the council turned down the idea. After all, once in power, they simply would not give up their privileged positions of "representing" their fellow students for anything. And herein lies the precise reason why LD has not yet unveiled any feasible economic opportunity: Political representatives are not really *representatives*, but rather, a time-limited special class with access to privileges, power, and connections to foster their career.

The Google Votes experiment, which ran from 2012 to 2015, was about engaging the Google staff in making decisions on trivial matters, such as which food they would like their canteen to serve or which logotype they fancied for a given project. This project was mainly about

[4]The reasons for the transformation have nothing to do with LD as such. The organization struggled to start due to issues with securing funding. Later, the initiator moved abroad and gave up the project, hence Župa was never tested for real.

participation in decisions that affect the community, rather than about the democratic control of power in an organization. For example, to choose which food they would prefer on the menu, employees would rank a selection of dishes according to their preferences. The system then, deploying the Schulze method (Schulze, 2011) for ranked voting, would select the most popular dish. Over the course of three years, 15,000 Google employees cast 87,000 votes; among these, 3.6% were delegated votes (Hardt and Lopes, 2015).

So far, only the German Pirates have managed to establish a significant LD culture and genuinely use it. This fits the ideology of the Pirates, and besides, at the time when LD was introduced, the German Pirates were a small, "insignificant" association. According to Jabbusch, LD had been a priority for the German Pirates since their formation and developed into a widely debated issue in the years 2007–2009.

3.5.2 The Path Down the Rabbit Hole: How the Pirates Did It Wrong

In 2009, the Pirates experienced nationwide publicity and a strong rise in membership. This rise in strength gave opportunity to focus on development, and several working groups were founded to investigate how to introduce advanced collective decision-making approaches for interparty decision-making processes. One such group founded the association *Liquid Democracy e. V.*, which developed the software *Adhocracy* that was later used by the German Bundestag (parliament) for an e-participation pilot (Bundestag, 2013). *Adhocracy*, however, did not utilize LD's transitive delegation principle. Also, as the Pirates found, *Adhocracy* did not entirely suit their requirements; consequently, within 2 weeks the LQFB system was developed (Jabbusch, 2011, p. 42), which continued playing a vital role in the party's policy-making process.

LQFB has been designed as a virtual arena for forming opinions by the party base, which are to serve the party bodies as recommendations and feedback (Jabbusch, 2011, p. 53). Opinion forming in LQFB takes place through *initiatives*, which can be proposed by any registered member—however, no discussions are permitted in order to prevent *trolling* (counterproductive contributions). Once an initiative has been proposed, it must first receive support from at least 10% of the registered users within a given time frame. If it succeeds in doing so, time for discussion and eventual modifications of the initiative is allocated, in which modifications are allowed, again, only within a given time span before the discussion period ends.

After this, members can vote on the final proposal. The interesting point here is that discussion is deliberately excluded from the system and thus has to take place in wikis, other forums, or in real-world debates (Jabbusch, 2011, pp. 58–60).

The party base uses LQFB to form *opinions* (*Meinungsbilder*). Jabbusch demonstrates how an *opinion* is formed using the example of the *universal basic income* (UBI), a political idea that the state should unconditionally give every citizen an income which covers all basic living costs. Forming of such an *opinion* is initiated by a proposer posting an *initiative*; each *initiative* can receive counter-*initiatives*, which are then competing within the *opinion* for dominance. It may happen that many *initiatives* within an *opinion* are accepted, which can result in a distorted representation of the party base's opinion. In addition, it is possible to initiate many similar *opinion*-forming processes, which further diversifies the results. At the time of Jabbusch's report, seven UBI-related *opinions* were formed. By the summer of 2013, more than 10 other *opinions* on this very topic existed. Despite the fact that it is up to the party leadership about how to consider the opinions and petitions from the base during their mandate, the *opinions* are further processed in party meetings and committees and are eventually included in official policy documents (or not). In the case of the UBI, the leadership accepted a petition for supporting a demonstration, which the party did by publishing an appeal for support on YouTube.

This kind of collaborative opinion gathering as exercised by the German Pirates is no more than an, admittedly, elaborately structured form of deliberation. The nonbinding nature of the *opinions* does not prevent the party leadership from acting against the will of the party base, as indeed had happened in 2013 when the decision of the party base was ignored by the party leadership (Herwatz, 2013). However, even if the party leadership were formally bound to the collectively expressed will, the Pirates might run the risk of inviting a torrent of different interpretations, contradictions, and juridical tricks that would allow the leadership to have its way in the end, one way or the other.

REFERENCES

Bitsch Link, J.A., Tchorbadjilski, A., Wehrle, K., 2014. Opportunistic vote delegation for e-voting based on liquid democracy. In: Proceedings of the 6th Extreme Conference on Communication. Presented at the ExtremeCom '14. ACM, Galapagos Islands.

Blühdorn, I., 2007. Sustaining the unsustainable: symbolic politics and the politics of simulation. Environ. Politics 16, 251–275. https://doi.org/10.1080/09644010701211759.

Blühdorn, I., 2014. Post-ecologist governmentality: post-democracy, post-politics and the politics of unsustainability. In: Wilson, J., Swyngedouw, E. (Eds.), The Post-Political and Its Discontents: Spaces of Depoliticisation, Spectres of Radical Politics. Edinburgh University Press, Edinburgh.

Blum, C., Zuber, C.I., 2016. Liquid democracy: potentials, problems, and perspectives. J. Polit. Philos. 24, 162–182. https://doi.org/10.1111/jopp.12065.

Bovens, M., Zouridis, S., 2002. From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control. Public Adm. Rev. 62, 174–184. https://doi.org/10.1111/0033-3352.00168.

Boyd, O.P., 2008. Differences in Grassroots Parties' e-Participation Systems. Örebro University.

Bundestag, 2013. Internet Enquete zieht nach drei Jahren Bilanz [Select Committee Sums up Activities of the Last Three Years]. Deutscher Bundestag.

Cringely, R.X., 2016. Apple vs. the FBI isn't at all the Way You Think It Is. BetaNews.

Downing, A., Molloy, B., n.d. Polly [WWW Document]. https://github.com/ppau/polly. (Accessed 9 June 2014).

Green-Armytage, J., 2010. Voluntary Delegation as the Basis for a Future Political System. University of California, Santa Barbara, CA.

Hainisch, R., Paulin, A., 2016. Civicracy: establishing a competent and responsible council of representatives based on liquid democracy. In: Proceedings of the International Conference for e-Democracy and Open Government 2016. Presented at the CeDEM'16: Conference for e-Democracy and Open Government. IEEE, Krems, Austria, pp. 10–16. https://doi.org/10.1109/CeDEM.2016.27.

Hardt, S., Lopes, L.C.R., 2015. Google Votes: A Liquid Democracy Experiment on a Corporate Social Network. Technical Disclosure Commons, Berkeley, CA.

Hennig-Thurau, T., Henning, V., Sattler, H., 2007. Consumer file sharing of motion pictures. J. Mark., 71 (4), 1–18.

Herwatz, C., 2013. Vorstand ignoriert Basis-Votum—wie demokratisch sind die Piraten? [Presidency Ignores Party Base: How Democratic are the Pirates?] [WWW Document]. n-tv.de. http://www.n-tv.de/politik/Wie-demokratisch-sind-die-Piraten-article10233026.html.

Jabbusch, S., 2011. Liquid Democracy in der Piratenpartei—eine neue Chance für innerparteiliche Demokratie im 21. Jahrhundert? [Liquid Democracy in the Pirate Party—a New Chance for Interparty-Democracy in the 21st Century?]. Universität Greifswald, Philosophische Fakultät, Greifswald.

Katz, E., 1957. The two-step flow of communication: an up-to-date report on an hypothesis. Public Opin. Q. 21, 61–78.

Lenarčič, S., 2009. Prenova sistema MFERAC [Rennovation of the MFERAC System]. In: Z inteligentnimi sistemi do strateške prednosti. Presented at the DSI 2009. Slovensko društvo informatika, Ljubljana.

McCarthy, S., 2013. Demystifying complexity: why worse is better in voting. SSRN Electron. J. https://doi.org/10.2139/ssrn.2342701.

Meinrath, S.D., Losey, J.W., Pickard, V.W., 2010. Digital feudalism: enclosures and erasures from digital rights management to the digital divide. CommLaw Conspect. 19, 423.

Nijeboer, A., 2013. Liquid Democracy Versus Direct Democracy Through Initiative and Referendum: Which Is Best? Democracy International, Cologne.

Norbäck, P., 2014. How the Democracy Experiment Ended. A Failure or Success? https://pernor.wordpress.com/2014/09/16/how-the-democracy-experiment-ended/. (Accessed 26 August 2018).

Oosterveld, W.T., de Spiegeleire, S., de Ridder, M., Sweijs, T., Bekkers, F., Polackova, D., Ward, S., El Din Salah, K., Rutten, R., Olah, N., 2015. Si Vis Pacem, Para Utique Pacem. The Hague Centre for Strategic Studies, The Hague, Netherlands.

Orwell, G., 1949. 1984. Secker and Warburg, London.
Paulin, A., 2010. Župa—Grassroots E-Democracy Revolution on the Web. In: Parycek, P., Prosser, A. (Eds.), Proceedings of the 4th International Conference on e-Democracy, books@ocg.at. Presented at the EDem2010. Österreichische Computer Gesellschaft, Krems, pp. 113–123.
Paulin, A., 2014. Through liquid democracy to sustainable non-bureaucratic government—harnessing the power of ICTs for a novel form of digital government. JeDEM 6, 216–230.
RS-AC, 2011. I U 1589/2010.
RS-IP: Informacijski Pooblaščenec, 2010. 090-150/2010/6.
RS-IP: Informacijski Pooblaščenec, 2012. 090-150/2010/38.
RS-MF: Ministrstvo za Finance Republike Slovenije, 2010. 090-22/2010/2.
Schulze, M., 2011. A new monotonic, clone-independent, reversal symmetric, and condorcet-consistent single-winner election method. Soc. Choice Welf. 36, 267–303. https://doi.org/10.1007/s00355-010-0475-4.
Swierczek, B., 2014. Five years of liquid democracy in Germany. Liq. Democr. J. 1, 8–19.
Tryhorn, C., 2009. Telegraph Paid £110,000 for MPs' Expenses Data. The Guardian.
van Hulten, M., 2014. Democratisation of the World: Do we Need a Global Parliament? http://blog.hulten.org/essays/global_democracy.pdf. (Accessed 26 August 2018).
Velikanov, C., 2013. О демократии обыкновенной, прямой и электронной [On traditional-, direct- and e-democracy]. Otchestvennye zapisky 57(6), 203–230.
Vivyan, N., Wagner, M., Tarlov, J., 2012. Representative misconduct, voter perceptions and accountability: evidence from the 2009 house of commons expenses scandal. Elect. Stud. 31, 750–763. https://doi.org/10.1016/j.electstud.2012.06.010.
Voss, O., 2013. Die fünf Probleme der Piraten [The Five Problems of the Pirates]. Wirtschaftswoche.
Zolleis, U., Prokopf, S., Strauch, F., 2010. Die Piratenpartei—Hype oder Herausforderung für die deutsche Parteienlandschaft [The Pirate Party—Hype or Challenge for the German Party Landscape]. Hanns-Seidel-Stiftung, München.
Zwattendorfer, B., Hillebold, C., Teufl, P., 2013. Secure and privacy-preserving proxy voting system. In: Proceedings of the 10th International Conference on E-Business Engineering. Presented at the 10th International Conference on e-Business Engineering. IEEE, pp. 472–477. https://doi.org/10.1109/ICEBE.2013.74.

This page intentionally left blank

CHAPTER 4

Governing Through Technology and the Failure of Written Law

Contents

Public action has always been controlled by legal systems, based on law expressed in written language. This law provisioned the existence of institutions; gave them written mandates to pursue the delivery of public services; and arranged safeguard institutions, such as inspectorates, courts, and other institutions of law enforcement, into cascading systems of checks and balances to govern the systems of the public apparatus. Law, which is expressed in natural language, is well suited to serve as a system that gives instructions to human organizations, or to individuals, to this end. It is well suited to describe the tasks and duties of a minister, to describe which behavior should be sanctioned by law, and to describe the confines of penalties if they are to be enforced. The message (the command) of the lawmaker is thus stored in the form of text, for someone to recover in its written form and to apply (Fig. 4.1). The communication of these commands is directed at human beings.

While it is perfectly suited to regulate human behavior, natural-language law is completely unsuited to give instructions to technical systems. Much as one cannot reason in BBC English with a stubborn mathematical equation, one will not find luck in convincing a machine to behave as desired

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00004-2

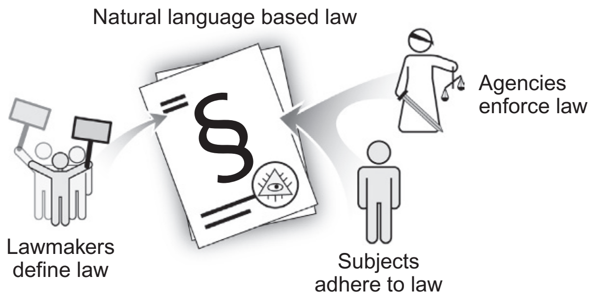

Fig. 4.1 Law expressed using natural languages can be understood by its (human) stakeholders.

by talking to it.[1] For this very reason, the *writing down* of law in a natural language for later retrieval and application by human agents, as humankind has done since before the Code of Ur-Nammu (the oldest known law code), cannot be applied to technical agents. Instead, *written-down* law must be reinterpreted and translated into a system which technical agents can natively understand and apply. This changes the situation in Fig. 4.1 to a situation as depicted in Fig. 4.2—the lawmaker, who previously was the ultimate source of (written) law, has given way to the system engineer, who now has the last say in how law (as expressed in the form of system architecture) is shaped.

Law is thus no longer controlled by any single point of power, but is increasingly trapped in black-box systems, which can be controlled neither by legislators nor by law enforcement agencies, not even by external system engineers. The *machines* which execute law translated into machine code thus become technical fortresses over which traditional mechanisms of control will have lost any possibility for control.

The result is a rift between law and technology, with traditional law existing on one side and technology on the other. Instead of finding a way to coexist, both disciplines seem to drift further and further apart. The remainder of this treatise further explores which options there are for legislative systems and technical systems to align themselves into a prosperous coexistence.

[1]The author is aware of the existence of artificial intelligence, language recognition, and similar fields of research and design, which aim to provide voice user interfaces, or which aim to recognize the meaning of a piece of writing. However, these fields address recognizing commands and approximating them to hard-coded routines existing in the machine at stake.

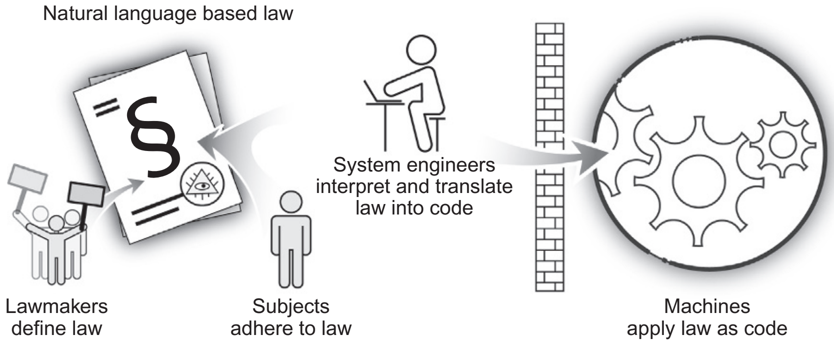

Fig. 4.2 Natural-language law must be translated to machine code to be executed by technical agents.

This chapter deals with two challenges within the domain of this *legal-technological rift*: the black-box nature of technical systems, which fosters unsustainability, clientelism, and legal uncertainty, will be discussed in Section 4.1; Section 4.2 discusses the ambiguity of written legislation when addressing technological systems or commanding their existence; Section 4.3, finally, delves deeper into the levels of technology, which contemporary law fails to address.

4.1 UNSUSTAINABILITY OF E-GOV: LEGAL (UN-)CERTAINTY, MONOPOLIZATION, EXCLUSION

When IBM coined the smart city buzzword, they managed to position themselves as an *obligatory passage point* for technology in the context of urban governance. Another such example is the United Nation's e-Gov ranking,[2] in which they set the general standards, which states then strive to fulfill. In both the cases of the e-Gov rankings and the smart city hype, the addressed public apparatuses reacted impulsively by jumping on the bandwagon and venturing into building a variety of online systems—more often than not simply to remain in competition with other cities and states. This "me-too" mentality has led to a *jungle of e-Gov* artifacts. The pressure to follow trends has resulted in hastily built e-Gov systems which are often no more than an end to themselves.

[2]The UN e-Gov surveys are the longest standing series on e-Gov progress around the world. The first report was produced in the year 2001, while the latest (as of 2019) was produced for the year 2018. Reports were produced for the years 2001, 2003, 2004, 2005, 2008, 2010, 2012, 2014, 2016, and 2018 and can be accessed from: https://publicadministration.un.org/en/Research/UN-e-Government-Surveys.

The crux of this *e-Gov jungle* is that it is not a system of systems, as it would be desirable in theory (this is where the *transactional stage* of e-Gov comes in), but rather an arbitrarily grown set of larger and smaller repositories, interfaces, and Web presences, each of which represent some fiefdom for a bureau to reign. The maintenance and evolution of these systems impose huge costs, which, if the systems are to remain, drain resources from the public apparatus. Once funding stops, the system becomes yet another ruin in the e-Gov jungle in the form of a nonfunctioning system, broken link, or outdated registry.

The manifold problems of the existing approaches to building e-Gov systems are known as the *three hazards of e-Gov* (Paulin, 2013): (I) the intrinsic expiration date of IT e-Gov artifacts, (II) implied monopolization and exclusion of competition, and (III) nonadherence to the principle of legality. These hazards lead to the conclusion that modern e-Gov must not be seen as a sustainable solution, but rather as a pioneering approach before some such sustainable solution can be engineered.

4.1.1 Hazard I: The Expiration Date

It goes without saying that at the design time of an e-Gov system, only then-valid laws can be taken into consideration (it is impossible to predict which regulations will be in force in the future) and, hence, changes in law will require a change of such a system. The entanglement between the law and the technical systems built to digitalize procedures and functionality mandated by the law can be dealt with in three different ways: a change of law can lead to a reengineering of the system, the old system can be replaced with a new one, or law can be mandated to the technology so that law is adapted to fit technology. Here are a few examples.

In 2009, in Slovenia, a new e-Justice system was published to handle the insolvency proceedings according to the *Financial Operations, Insolvency Proceedings, and Compulsory Dissolution Act* (ZFPIPP[3])—the then-valid law. In this system (Bezeljak, 2009), users can use pre-prepared PDF templates of forms required for actions in legal proceedings to interact with the system through dedicated user interfaces. They can use this system to enter data, electronically sign the documents, and to verify such signatures. They can also use this system for retrieving data from Web services offered by other

[3] *Zakon o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju*, SOP 2007-01-6413.

e-Gov systems. The ZFPIPP was enacted in 2007 and underwent approximately 10 changes between 2009 and 2013, a few of them due to ruling by the Slovenian Supreme Court. There are no reports of how strongly these changes of ZFPIPP influenced this e-Justice system; however, it is very likely that certain parts of this highly complex e-Gov system became legally obsolete and that they had to be reengineered.

Peled (2014, chap. Introduction) points out this problem of perpetually changing law in the case of the US Internal Revenue Service (IRS):

> *Since the 1954 overhaul of the U.S. Internal Revenue Code, Congress has passed 238 additional tax laws. Because tax laws are not retroactive, IRS programmers have created and continue to maintain multiple annual tax 'versions' of the entire Internal Revenue Code [...] Moreover, tax laws often have an effective duration after which they expire. So, each annual software layer inside the IRS electronic mountain must know which information elements to 'borrow' from other historical layers and how to correctly use the borrowed information.*

IRS' "electronic mountain" (Peled, 2014) has been built for decades, using COBOL, a programming language that was popular in business and government circles between the 1960s and the 1980s. By the end of the 1980s, this language was already considered to be falling into decline. Given the strong reliance on COBOL by these antiquated government IT infrastructures, this language is tolerated still in the 21st century, albeit no longer as a part of modern university curricula.

In Montenegro, in 2011, a population registry was designed to integrate various administrative proceedings as individual workflows pertaining to the then-valid law (Horvat, 2011). During the requirements-analysis phase, the team found discrepancies in the law which made it impossible to engineer the system as desired. To overcome this, the law was changed such that the system could be designed. Needless to say, future lawmakers will face a system *too big to be changed* that will severely impact their freedom in drafting new legislation.

Slovenia's market inspectorate received a completely reengineered system in 2009, which was needed due to the large number of changes in different acts (Naraks and Golob, 2009). The result was a full-fledged document management system with over 200 predefined templates that either fully or partly automatized different administrative workflows. The system was designed to be extendable so that future workflows could be added at runtime. Nevertheless, the authors noted that further updates and adaptations would be required to keep the system fit for use as the law changed.

Fluctuating legislation is a particular challenge when designing e-Gov systems. When a public procurement management system was developed in Slovenia, the development team reported severe challenges with the continuously changing legislation (Kolar, 2009) during the process of development. Another challenge was found when interacting with the public administration officers—as they were indignant about having to deal with a new system, many excuses were brought up which obstructed the development. By 2009, when the system was already in an advanced stage of use, the developers came to the conclusion that the system was already in need of renovations, updates, and readjustments due to changes in the law.

Even seemingly harmless cases tell a story of e-Gov decay, such as the case of Slovenia's central dog registry. Established in 2000, due to changes in national and EU legislation in the first 8 years of operation, a new registry had to be engineered by 2009 (Kos and Zorman, 2009). Among the key reasons for the development of the new system were, the obsolete technology of both the back and front ends, an inefficient data model, missing connectivity to other vital registries, and unfitness to respond to changes in veterinary practice and regulations.

In 2011, the management of Slovenia's treasury was massively reengineered. Before the reengineering, a multitude of heterogeneous e-Gov systems managed the public finances; however, these failed to provide sustainable functionality. Thus, between 2007 and 2010, a unified system was developed and engineered, whose development (in terms of functional adaptations and updates) continues into the future.

Another such simple, though perhaps common, vulnerability of e-Gov systems is the case of US Department of Defense's embarrassing situation in 2005, when the *Federal Republic of Yugoslavia* changed its name to *Serbia and Montenegro*. As the development and maintenance of their back-end systems was outsourced to another company, which was bound to a strict system update schedule, the United States was not able to use the new name in official communication until the next scheduled update of the system (Burton, 2011).

A final example comes from our own 2014 to 2016 observations of a governance system in use at the Vienna University of Technology, which was used to administer the course duties of a large number of students. The system was developed to keep track of student activities, make assessments of their performance in given assignments, providing statistics and insights into individual student's curricula, and the like. The system was developed several years prior by technical staff and at that time was tailored to fit the needs of a single member of staff. The functionality of the system was thus fixed to a single defined workflow of how to manage students throughout their participation in the course. As new staff joined the team, bringing in new views and experiences, demands for modifications of the system's functionality reached the developers, which were met with objections and resulted in conflicts. The new staff requested access to the underlying databases and the code itself in order to take development into their own hands, which, however, was rejected by the developers for fear of losing their monopoly on the situation. A solution was found by dismissing the technical team and appointing a new one, which developed a new system. But this solution did not solve the problem that the academic staff remained dependent on a technical team's availability and cooperation. In this particular case, the system did not expire due to changes in legislation, but rather due to changes of requirements. Nonetheless, this boils down to the same issue: *the system expires once the context changes*.

The implied expiration date of e-Gov systems is a crucial factor of their unsustainability. This factor is not the only hazard of e-Gov, but unlike the other two, which will be described further below, this one is very easy to understand. Each user of an e-Gov system can observe how changes occur themselves, as these changes reflect in changed user interfaces, changed functionality, and so on.

4.1.2 Hazard II: Monopolization and Exclusion

In the case of the university course described above, the system developers managed to make themselves indispensable. Thus, even though they were formally subordinate to the academic staff, they managed to become more powerful. As they had a monopoly on the technical knowledge for maintaining and updating the technical system that was required for administering student's duties and administering, correcting, and grading tests, they were in a position where they could dictate the modalities of maintenance and flow of work. They stubbornly refused to hand over this know-how and the underlying code—after all, they could not be confident that their positions would remain relevant once the academic staff gained control of the system. Ultimately, the academic staff could only dismiss the developers and let somebody else develop a new system.

In this case, the academic staff lacked the motivation to interfere with the developers and left them in control of their sinecure. The staff benefitted greatly from the systems created by the developers, as it allowed them to efficiently cope with the large workload that could otherwise not be managed.

This *modus operandi* corresponds to what the German sociologist Luhmann termed *useful illegality*[4] (Mayr, 2011, p. 44), i.e., a situation in which an organization deliberately *does not* operate by the book, as it is mutually beneficial to go against formal rules, relations, and regulations.

As Walter (2011, p. 44) discusses, this kind of useful illegality plays a vital role in stabilizing state bureaucracies, as it can fill gaps in legislation in order to allow agencies to operate in accordance with their core missions. Filling such gaps, which span between what the legislator has defined and what the state agencies are commissioned to deliver, is an unavoidable task when it comes to e-Gov systems. While legislators merely define the gross functionality of the systems, the details of the concrete implementation, which are crucial to bring the systems to life, are shifted implicitly to the system designers and developers.

Bovens and Zouridis (2002) emphasized the role of *useful illegality* in the context of e-Gov systems. Rather than referring to it as e-Gov, they call the technization of public administrations *system-level bureaucracy*, which in essence corresponds to the transactional stage of e-Gov (see p. 43), i.e., the situation in which interconnected e-Gov systems are capable of generating administrative decisions with no, or very little, human intervention. They emphasize that a new class of politically unauthorized people, such as system designers, legal policy staff, and IT experts, gain "discretionary power to convert legal frameworks into concrete algorithms, decision trees, and modules" (Bovens and Zouridis, 2002). While this new class of politically unauthorized "ad hoc bureaucrats" can play a beneficial role (i.e., "getting things done," in terms of useful illegality), they do contribute to making e-Gov systemically unsustainable by becoming indispensable and thus excluding competition.

To illustrate the hazard of monopolization and exclusion within e-Gov systems, we discuss three examples: The European e-ID landscape, the Austrian *Bürgerkarte* e-ID system, and the Slovenian SVEV system for secure electronic delivery. In all three cases, there is a concrete legal basis which defines (and mandates) the *existence* of technical artifacts in the highly sensitive domain of electronic identification, authorization, and signing. However, the law did not clarify *how* these systems should be constructed from a technical perspective and omitted other crucial characteristics—Section 4.2 will take a closer look.

[4]Brauchbare Illegalität.

Electronic identity (e-ID) technologies have received significant worldwide attention in the years around the turn of the millennium. From a technological perspective, e-ID is the realization of the principle of public-key cryptography, where a cryptographic algorithm utilizes a pair of entangled keys—a public one (which can be openly known to anyone) and a private one (which is known only to the person who is encrypting this piece of information). These two keys are linked mathematically in such a fashion that it would be unreasonably difficult (e.g., it would take thousands of years) to guess the private key if the public key was known. Information which has been encrypted using the private key can be easily decrypted by means of the public key (or vice versa), and by this, the information can be definitely linked to the holder of the private key. An alternative use of this principle is for digital signing (the holder of the private key encrypted a token such as a "hashed" message, which is algorithmically linked to the original message) or identification, whereby an identification provider signed a certificate, which can be used for purposes of trusted identification. e-ID technology will usually serve the purposes of both identification and digital signing.

To boost the IT industry and adjacent ecosystems, legislation mandated the existence of the electronic signature (e-Sig), which was to have equal validity as the handwritten signature in the face of law. A crucial milestone for legally significant electronic interaction in the European Union was Directive[5] 1999/93/EC. Implementation of this directive into national law should have been realized before July 19, 2001. Although the directive explicitly focused on e-Sigs, the other aspects, namely identification, authentication, and thus the regulation of e-ID, were implied (Myhr, 2005). Directive 1999/93/EC was deliberately designed to be technology- and vendor-neutral in order to protect the European single market from regulative tendencies of national states (Dumortier, 2004). Further, a temporary electronic equivalence to the legal concept of handwritten signature—the qualified electronic signature (Qe-Sig) (also technology-neutral)—was also defined so that in cases where legal code required a "handwritten signature," this requirement would be satisfied by that type of e-Sig (Dumortier, 2004).

[5]European directives are the source of European legislation—they normalize legislation throughout all of the European member countries. Effectively, this means that a subject (citizen or company) needs to have knowledge about the content of the directive and can directly refer to it before legal proceedings. The national law must completely incorporate the provisions of the directives, and national courts must not rule against them.

As the directive strongly focused on establishing a regulation that would be technology- and vendor-neutral, it failed to provide clear definitions on which technology to use for creating and verifying e-Sigs. Governments, which wanted to imminently provide electronic identification and signing as part of their e-Gov systems, went on to sponsor providers of national technological solutions, who later became monopolists in providing technology that complied with the requirements of national e-Gov systems. This led to the rise of a number of heterogeneous, national e-ID providers, whose reach was confined to the national borders of their respective national state, which is not compliant with the foundational European ideal of border-free movement and business.

On the basis of Directive 1999/93/EC, a European "Babel" of mutually incompatible national e-ID systems emerged, in which the e-ID issued by one member state's national provider was not accepted by another member state's e-Gov system. In order to overcome this problem, the European Commission funded the STORK project, which aimed to create an interoperability solution in the form of a middle layer, and which would translate between the respective national solutions of the participating member states. However, the project was confined to the level of piloting, was limited to concrete applications, and failed to provide a systemic solution to the problem of lack of mutual recognition of electronic identification and signatures across borders.

The Austrian national e-ID, the *Bürgerkarte* (*citizen card*, CC), is a highly sophisticated and globally unique mechanism for providing identification, authorization, and signing, designed for the online interaction between citizens and government agencies. Unlike other European national identification schemes, which often rely on smart-card technology (Arora, 2007; Rissanen, 2010), the Austrians chose a technology- and vendor-neutral approach for the CC. In fact, the CC is not a concrete technology, but rather only an abstract legal concept defined as "a logical unit, which regardless of its implementation binds a qualified e-signature with the *Identity-Link*." The *Identity-Link* is a small piece of information—an "assertion," stating the identity of a person. This concept is likewise a legal one with a technical instantiation born out of the legal-technical vacuum of the Austrian law.

Several technical recommendations that regulate the features of the CC have been designed; however, these have not been issued by any politically empowered body and are consequently not binding by law. Besides, using the CC is only optional. Austrian legislation merely requires that access to sensitive personal data from a public registry is granted only to unambiguously identified requesters, provided that the request can be unambiguously authenticated; proof for both must be given in electronic form. In principle, technologies other than the CC can also satisfy these legal provisions. But then again, these conditions, as luck would have it, are automatically fulfilled by using a CC, and hence, the CC is not only recommended but also the only mechanism for identification, authentication, and signing that one can use with Austria's e-Gov services.

As Austria is a member state of the EU, it must not discriminate against other providers of e-ID technologies from the EU that comply with the directive. However, the Austrian e-Gov services only factually support the CC as implemented by a single national provider that is closely personally and professionally linked with agencies that regulate the Austrian e-ID landscape (Paulin, 2012). The Austrian e-ID landscape is thus controlled by a network/clan, which provides their services as a monopoly and prevents national alternatives or foreign providers from offering their services in Austria.

There is little information available about cases in which independent providers have attempted to challenge national monopolists in order to get their own solutions accepted by national e-Gov systems. An isolated case of such an attempt, however, has been documented in the scope of the Slovenian electronic delivery framework SVEV (RS-AC, 2011), as shall be described below.

The background of the Slovenian case is similar to the one of the European e-ID: legal provisions for submitting applications electronically were first enacted for administrative proceedings in 2006 and later for civil legal proceedings in 2007. Both almost identically regulate that applications in electronic form are sent electronically to the information system of the addressee, which automatically confirms the receipt of the message. However, a detailed definition of such an "information system" has been omitted. To make matters worse, both laws contain provisions that allow subjects to actually *demand* delivery in *electronic form*, whereby specialized electronic delivery providers should deliver messages into the addressee's *secure electronic mail box*, which, however, is not defined in detail either by law or by bylaws (Paulin and Welzer, 2013).

In the case of the Slovenian electronic delivery framework and the European e-ID, informal clans are the drivers behind local legislative activities, which enable privileged technical solutions to assume monopolistic roles in domestic markets, through which those clans secure the development and maintenance of their own technical solutions to the disadvantage of outsiders.

4.1.3 Hazard III: Legal Certainty

Legal theory distinguishes between public law and private law, whereby public law regulates the relations between the state and its citizens—ergo, relations between the sovereign and its subjects—while private law regulates relations amid the subjects based on their will (Horwitz, 1982; Toplak, 2008, p. 23). A major difference between public and private law is that private law *restricts* the *freedom* of the subjects, while public law *empowers* the sovereign. In societies that adhere to the rule of law, the sovereign (ergo, the political bodies of the public apparatus) operates in accordance with the principle of legality, which means that every action and every decision made by the state must be explicitly defined by law. This applies both to stated decisions and to the procedures that lead to them (Jerovšek, 2000). This fundamental legal principle not only allows subjects to exercise control over the sovereign, but also guarantees legal certainty—the sovereign's actions are transparent and foreseeable. Legal certainty prevents the state's bodies (e.g., government, police, and courts) from acting or deciding arbitrarily, which is crucial, as state despotism would break core legal principles, such as the principle of equality before law (Šinkovec, 1998, p. 31).

e-Gov, however, challenges the principle of legality, as it delegates government *behavior* to e-Gov systems, hence machines. This might not seem to be an issue at first glance, and authors such as Bovens and Zouridis even argued that from the perspective of equality before law, e-Gov (there, system-level bureaucracy) "may be regarded as the zenith of legal rational authority [as] thanks to ICT, implementation of the law has been almost wholly disciplined" (Bovens and Zouridis, 2002, p. 181).[6] But does e-Gov really make procedures perfect?

From a technical perspective, functionality offered through e-Gov systems often contains procedures which subjects can initiate (and communicate with) remotely, whereby such procedures are executed on the server of the particular agency. The communication between the subject and the sovereign (represented by the agency) is thus channeled through technical communication between the technical equipment of the subject and the serving terminal of the sovereign. Unlike human-to-human communication, which is based on the interpretation of analog messages (voice, text, body language, …), digital communication is discrete, exact, and unambiguous. Human communication, for example, does not rely on strict grammar

[6]Bovens and Zouridis also clearly emphasize the issue with the uncontrolled delegation of discretionary power, as described in the context of e-Gov hazard II above.

or correct pronunciation of words—two foreigners will be able to perfectly communicate in English despite their ignorance of its grammatical rules. Likewise, general human perception is based on the interpretation of analogue, ambiguous information—e.g., we can visually recognize a car even though we have never seen it in the exactly same environment, shape, angle, etc. On the other hand, it is impossible for two computers to communicate without adhering to strict protocols that regulate the exact semantics of the transmitted signals and information. So, when we say that human interaction is analogue and computer interaction is digital, we imply that the former is ambiguous and therefore must be interpreted, while latter is unambiguous and precise by definition.

e-Gov, too, should comply with the digital nature of machine-to-machine interaction, which is another concern in the realm of legal certainty. In the real (analogue) world, interactions are subject to interpretation, and hence, legal certainty can be achieved by defining spaces of discretion within which interaction takes place. An administrative proceeding, for example, is initiated by submitting a written and signed application to the responsible government agency. The fine details of the message are a matter of discretion—it does not matter on which material the application is written, it does not matter which font is used, nor is there a need for exact wording in the application. Since the interaction takes place in an analogue dimension, it is expected that the addressee will be able to understand the request. On the other hand, any digital request sent to a digital system must follow a clear and unambiguous protocol that rigorously defines the rule of the structure and the rule of the semantics.

This, then, is something new. Law has always governed only the relations between human beings—by limiting the freedom of its subjects, the sovereign has regulated their behavior. To regulate behavior, Lawrence Lessig (2006, chap. 7) identifies four constraints: laws, social norms, the market, and architecture. *Law* regulates by ordering people to behave in a certain way while threatening noncompliance with punishment—e.g., we may drive our car on the highway only within a certain speed limit, or else we risk getting fined. *Social norms*, too, resort to threatening with punishment (e.g., social isolation), but unlike laws they are not imposed "top-down" by the authority (by the sovereign), but rather evolve from within the community itself—e.g., loud neighbors might be scorned by the other neighbors for their disturbing behavior. *Markets* regulate through the offer/demand ratio; influence by the sovereign can be exercised, for example, by forbidding the import of certain goods (e.g., drugs), or by imposing selective taxes.

The fourth modality is *architecture*, which regulates by constraining the physical environment. In the real world, these are streets which divide neighborhoods, bridges that connect riverbanks, or public squares where people meet. Regulation through architecture has also been applied in the form of broad boulevards in Paris to prevent uprisings (an effective mob requires density, which was easily achieved in the narrow alleys in old Paris (Lessig, 1999, n. 18)); to German state institutions by placing them in different cities—the High Court in Karlsruhe and the legislature in Berlin, in order to discourage corruption (Lessig, 1999, p. 507); and to curb child prostitution in Vienna where road barriers were placed on streets to prevent the cruising of clients in the infamous Stuwerviertel neighborhood (News.at, 2008).

Lessig aims to outline how cyberspace is regulated, unfolding his analysis based on the premise that cyberspace is ruled by the architecture of its "code." By "code" he means "the software and hardware that make cyberspace the way it is" (Lessig, 1999). There is a point in that—if anything rules the myriads of electronic messages that zip around the globe each second, it is neither law nor social norms, nor the market, but clear and strict architecture of the software and hardware systems through which they traverse.

But herein lies the main point of the third e-Gov hazard: If a user (the client) interacts with an e-Gov service, they must engage with an administrative proceeding with characteristics that are hard-coded within the architecture of the online system. The messages the client exchanges with the service's remote endpoint (the server) are exchanged following an implied protocol, which both the client and the server understand. To understand what's going on, we can take a detailed look at an exchange of messages. When a Web form is interacted with in the Web browser, the user first composes an HTTP[7] request (e.g., enters a Web address into the browser window); this is sent to the Web server of the e-Gov application's back-end system over the Internet. The server then responds by composing and sending an HTML[8] Web page, which the requester's terminal equipment (e.g., the Web browser) *may* (or may not) visualize and present as a user interface to the requester for further interaction. Over a series of such requests

[7]The *hypertext transfer protocol* is the standard protocol for communication with Web servers.

[8]The *hypertext markup language* is nowadays just one of many standards for digital documents. It was initially developed to semantically describe content accessible over the Web. The vast majority of Web pages use HTML.

and responses, the user interacts with the e-Gov service to achieve what they intend to do—e.g., renew their car registration. What is important to understand here is that the Web server (thus, the e-Gov system) has no influence on how the client treats the response, nor does it know whether or not the response was received at all.

The services which e-Gov systems provide, such as filing a tax return, registering a change of resident address, applying for social benefits, or accessing data from a public registry, all fall under the domain of public law. The exchange of messages—the user's requests and the server's responses in the interaction between the user and the e-Gov system—are thus administrative proceedings initiated by the user with the goal to influence their legal status or rights (cf. Chapter 6) or to be granted access to public information. From this perspective, it becomes evident that legal principles must also be applied to this dimension in order to assure legitimate, nondiscriminative access to e-Gov systems. Hence, in the same way that human officers are obliged to lead administrative proceedings in accordance with formal procedures that are transparent and public, so should the procedures by which e-Gov systems process and handle requests be defined in a transparent and legitimate way. Unlike in the analogue world, where it is sufficient to define the objectives of the key steps of formal proceedings, cyberspace requires an unambiguous definition of procedures, protocols, and also other details, such as the location of the systems within the Internet, due to its architectural principles.

The inability to know the exact protocol of interaction with an e-Gov service implies that one cannot harness the potential of the available online channel. On the other hand, if the protocol was clear and documented, one could derive added value by automatizing interaction, or by embedding the e-Gov service into a more complex solution. As an example, we can consider the tedious task of renewing the car registration year after year. If one could rely on the clarity of a standardized protocol for interaction with the respective national e-Gov service, an automated workflow could easily be set up and connected to a calendar app, which would trigger the car registration on a certain date. Alas, even though this would be the effect of a proper adherence to the principle of legal certainty—i.e., the reliance on the transparency and availability of a protocol—it is not part of any e-Gov system so far.

In order to assure genuine legal certainty of e-Gov systems, each system's internal architecture, processing logic, public interfaces of all kind, and so on would need to be carefully documented and legitimized by a politically authorized body. However, anyone who would be courageous enough to document and properly legitimize each and every technical endpoint, each communicational protocol, and each piece of code used in the existing e-Gov applications would end up facing a nightmare of endless recursion-like Sisyphus. It is not that achieving legal certainty with technical artifacts is impossible—Part III discusses this in more detail—it is simply that modern e-Gov systems have not been designed with legal certainty in mind. For this reason, e-Gov is also not sustainable if scrutinized from the perspective of core legal principles.

4.2 CHALLENGING LAW: THE AMBIGUITY OF THE WRITTEN WORD

The paradigm of the modern relation between the state and its subjects is one that largely gives the latter the benefit of the doubt. In fact, this is one of the objectives of the *rule of law* principle; the second being that the terms and conditions by which the state governs the public apparatus must be known in advance and laid down in comprehensive terms. This is reflected in the criminal code, where it is upon the state to prove one's guilt, and to some extent also in administrative and legal proceedings in which the ways of interaction are deliberately kept nonrestrictive. In this way, the criminal code provides all of the information one needs in order to stay out of jail, and the code on administrative and legal proceedings provides all of the knowledge one needs when interacting with the state.

With the introduction of technical systems for public governance, this principle, that the conditions of interaction with the state must be clear, slowly withers away. One's ability to read a legal code in order to understand all that is necessary to be able to lawfully interact with the state has been swallowed by the legal-technological rift, as the examples below shall demonstrate.

4.2.1 Slovenian Electronic Delivery

In Slovenia, formal interaction with the state is regulated by several distinct legal codes. One such code is the *General Administrative Procedure Act* (the ZUP), which regulates the interaction between citizens and the state in the case of administrative proceedings. Another code is the *Civil Procedure Act* (the ZPP), which regulates interaction with the civil courts. In both cases, the key element of interaction between the citizen and the state is the *application*, an expression of intent or desire, for which no particular form is prescribed for the citizen to adhere to. For all it matters, the citizen's applications can be expressed orally, or in writing, as long as the application's content is comprehensible to the receiving body of the state—it could be even chiseled in stone or written in one's own blood on a piece of wood. The wording is also irrelevant, as long as the information transmitted is clear and comprehensible.

This formlessness of these applications is important as it protects the subject from state despotism. Imagine an administration that would disqualify an application for trivial mistakes in filing forms, such as data entered in the wrong field or minor spelling errors. Or, for example, that the administration would reject a free-text application because the style of language or font used was not to the liking of the officer in charge. This would put the applicants in a position in which they would have to hope and pray that their application is accepted by the state. Unfortunately, modern e-Gov law does exactly that: it introduces state despotism, robbing subjects of the legal safety that trusting in the published law is supposed to provide. Following is an example from Slovenia, which focuses on the provisions of ZUP and ZPP in the context of legal and administrative proceedings, respectively.

When enacted in 1999 to replace the former Yugoslavian legislation, Slovenia's ZUP provisioned that an application must be filed orally or in writing, whereby if in writing, it can be handwritten, created using mechanographic means (e.g., using a typewriter), or "using electronic media."[9] These applications can then be sent to the addressee via postal service, through fax, or "through electronic media," if the addressee has the appropriate facility to receive such. These provisions remained in line with the doctrine to avoid restrictions on the design and form of the application. In a spur of modernization, the renovation of the ZUP in 2004 brought significant change in this regard—communication with the state using electronic means was now heavily governed. Where previously an application could be delivered through electronic media, the newly introduced "electronic application" now had to be signed using a Qe-Sig and a qualified certificate. This electronic application was then sent to the addressee through "electronic channels of communication," which had to be done by sending the application electronically to the addressee's "information system," or "the single access point for receiving applications"; the information system was then supposed to "automatically confirm the receipt of the application." Further details were to be defined by a special decree of the government.

[9]It is not really clear what is meant by electronic media. It might well refer to e-mail though.

Thus, the paradigm had radically changed. It was no longer possible to rely on the broad definition by the old ZUP in order to compose and submit an application in the form of an e-mail, fax, or other mechanographic means. It was now up to the government to provide the terms and conditions of interaction in the form of a decree. More than a decade since the implementation of ZUP, the decree mentioned in ZUP was yet to be enacted, and accordingly agencies which were obliged by law to adhere to ZUP (virtually any public-sector organization in Slovenia) routinely rejected electronic applications sent via e-mail under the pretext that they were not able to verify the e-Sig. Applicants were advised to file their applications via the national e-Gov one stop shop, which was interpreted to be the "single access point for receiving applications" as the law mandates. This in turn gave exclusive power to the system controllers to technologically limit the way in which stakeholders could interact with that system.

The story of ZPP is slightly more complex. The original ZPP was enacted in 1999, and, like the original ZUP, followed a very liberal and permissive policy with regard to electronic communication. It mandated that an application can be submitted via *telecommunication services*. In 2007, ZPP was updated to contain almost exactly the same provision regarding electronic communication as was introduced in ZUP in 2004. The wording was essentially the same as in ZUP, except that there was no "single access point for receiving applications" in this case. This law gave power to the government to define more detailed terms and conditions, although in this case, these were actually adhered to.

Following the mandate of ZPP, the government issued a decree, which described the existence of an e-Justice system, i.e., an information system that serves the administrative and organizational needs of the Slovenian judicative system. This system was described as consisting of five modules (a security module, a workflow management system, two registries—one to keep track of incoming and outgoing communication and the other to administer the individual files—and a system for administering certified deliveries) and a Web front end. To this end, the nation's e-Justice system was described as what it was: a black box.

This decree delegated authority to define concrete technical specifications needed to interface with the e-Justice system to the agency which hosted the e-Justice system. These specifications were then to be followed by providers of certified e-mail services. The full discretionary power was thus in the hands of the hosting agency, which controlled who was allowed to interface and who was not. Accordingly, the e-Justice system is a hotbed for neo-feudal arrangements. The realm of electronic delivery is firmly in the hands of networks, rather than subject to the rule of law.

The legislative foundation provided by the Slovenian decree that legitimizes the mentioned e-Justice system is similar to other national legislation that aims to legitimize the existence of black-box e-Gov (including e-Justice and e-Health) systems. The Austrian *e-Government Gesetz* (regulating the existence of the e-ID) and the *Elektronische Gesundheitsakte-Gesetz* (providing legitimacy for the ELGA national e-Health grid) both provide legitimacy for elaborate systems and infrastructures in the form of black-box systems. As these systems' technical functionality, their architecture, and their interfaces are defined by system designers and developers, rather than at the level of law, they remain out of reach of the rule of law.

For example, when law mandates that data should be stored, it only prescribes *what* is going to be stored and collected—this is sufficient to legitimize collection of data. However, law does not define crucial technical details that would be required to interact with such data by technical means. Specifically, law fails to define *how* (i.e., in which structure) or *where* (e.g., in which database) such data is stored. This might seem a nonissue at first, and from certain points of view, it is a nonissue—these details are of no relevance if the sole objective of legislation is to legitimize the existence of yet another black-box system. However, as discussed in Section 3.4, the issue of access to public data, among others, must be taken into account. Accordingly, unclear legislative definition of those data structures, which contain *data/information* falling in the domain of public data either now or will do so in the future, is a significant stumbling block to future application of the *freedom-of-information* (FOI) principle.

The result of modern legislation is black-box systems, which will be the future sinecures of too-big-to-fail agencies. This kind of law gives up the power to control and change these systems, as it fails to provide concrete technological levers to do so in the future.

4.2.2 European Electronic Identity: Unavoidable Monopolization

In the section on *monopolization and exclusion* (Section 4.1.12) as a core hazard to the integrity of e-Gov, we touched upon the European e-ID framework and its flawed implementation which resulted in national monopolistic providers. This section takes a closer look at the rift between technology and the written law and explains why they simply are unable to be compliant with each other.

Directive 1999/93/EC (EU-EC, 2000) defined the gold standard for e-Sigs, namely the Qe-Sig. The Qe-Sig is a legal analogue to the handwritten signature—i.e., whenever law uses the wording *handwritten signature*, the Qe-Sig satisfies this criterion. From a legal standpoint (Dumortier, 2004), this analogy is a temporary measure to be used while legislation using the terminology "handwritten signature" exists; future law should thus make use of *advanced electronic signatures* (Ae-Sigs). The Ae-Sig is defined as an e-Sig that reliably identifies the signer, has been created using *data* which the signer can keep under their sole control, and is bound to the *signed data* in a way that any posterior change of the signed data can be detected. The Qe-Sig is defined as an Ae-Sig created by a *secure signature creation device* (SSCD), based on a *qualified certificate*. The SSCD is defined as configured software or hardware used to handle signature creation data, whereby this software or hardware must comply with security requirements imposed by law. The *qualified certificate* is a *certificate* which contains specified data and which has been issued by a *certificate service provider* (e.g., a certificate authority). A *certificate* in turn is defined as an "electronic attestation which links *signature-verification data* to a person and confirms the identity of that person."

The above prescriptions provide a solid recipe for how an arbitrator can determine whether or not an e-Sig brought before them is a *qualified* one, or merely an *advanced* one, and whether or not a block of data can be interpreted as an e-Sig at all. There is, however, another side to this coin, and this is where the trouble starts: What exactly *are* these concepts? What is a *certificate*? What is an *SSCD*? What is an *e-Sig*? Let's take a closer look at what these ought to be, by looking at the e-Sig as such.

The e-Sig *may* (or may not) refer to the concept of digital signatures as used in the case of public-key cryptography. The vagueness at this early point in defining is already an issue. The Directive defines the e-Sig as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"—to this extent, it is the *context* in which the signature is applied that defines how the signature will look. This means that it is up to the particular technical system to define the *logical association of data* which it considers as an e-Sig within its own domain, and from which it authenticates the signatory. This definition allows an arbiter to recognize an e-Sig as one that adheres to the definition of the law after analyzing the context in which it is being used. Further, this definition also allows a systems developer to create a system that uses e-Sig for authentication. But this definition handicaps citizens in the use of e-Sig when interacting with parties who do not explicitly recognize its validity.

In practice, this meant, for example, that an e-Sig generated by technology that the Austrian government accepts was not accepted by the German state, and vice versa.

To escape this state of total vagueness, we may go ahead and assume that the e-Sig is to be understood as a digital signature which involves public-key cryptography. Public-key cryptography is a clear concept; it involves signing a digest of data with a secret cipher, which is mathematically linked to a public cipher that can then be used to verify the signature. But even so, the equation is one with too many variables. First, one needs to define the algorithm used to create/verify the signature: popular programming frameworks (e.g., Microsoft's .Net) offer around three different types of algorithms—the *Digital Signature Algorithm* (DSA), the *Rivest-Shamir-Adleman Algorithm* (RSA), and the *Elliptic Curve Cryptography Digital Signature Algorithm* (ECDSA). The documentation of a specialized cryptographic library,[10] the BouncyCastle library, which is available for the popular programming frameworks Java and .Net, provides more details into the complexity of the matter (bouncycastle.org, 2015). For elliptic curve cryptography alone, one can choose between ECDSA and ECGOST; support for ECDSA is further provided for the F_P curve and for the F_{2m} curve, each coming in several different standards, namely ANSI X9.62, SEC, and Teletrust in case of F_{2m}.

Given this large variety of approaches, the legislators of Directive 1999/93/EC failed to provide a clear definition of what they actually mean by the words "electronic signature." This detail, then, is only one of the manifold ambiguities of that particular regulation. Even though it might well be that it was never the actual intention to define the e-Sig as a clear technological concept, this case nevertheless demonstrates the challenges faced when legislation comes into contact with technology.

Directive 1999/93/EC was later repealed by Regulation (EU) No 910/2014, which was enforced as of July 2016. One of the reasons for this action was exactly the cross-border noninteroperability of European e-Sigs mentioned above. Even though the regulation did not substantially change the definitions of the terms at stake, it did instead entirely circumvent the challenge of defining the technical characteristics of the

[10]In programming, a library is a file that contains modules such as subroutines, which provide precoded software features that can be incorporated by programmers into the software they develop. This way, software developers can reuse components that can be provided by others to build complex software systems.

e-Sig. Instead, it provisioned a European registry of nationally accredited e-Sig providers, whose signatures had to be recognized across borders. This solution brought legislation back into a state where it was no longer interfering with the technology. Instead, discretionary power to define what constitutes the e-Sig was delegated to national institutions and interinstitutional agreements.

4.3 CHALLENGES OF MULTILEVEL ACCESS TO TECHNOLOGY

When modern law mandates which data is to be stored and collected, it does no more than legitimizing and governing the respective actions of the data collectors. The result of this limit of *written-down* law's power was reflected in two cases discussed so far: one was the problem of nonregulated interfaces for electronic interaction with the public apparatus, which we discussed as part of the hazard of legal certainty in Section 4.1.3; the other was the issue with access to public information discussed in Section 3.4. Both issues have the same roots, that is, the *legal-technological rift*, which restricts modern law from reaching out into the domain of technology.

When the Austrian *Führerscheingesetz* defines that "the datasets about the registered persons consist of: a) family name, b) first name(s), c) date and place of birth, [...], f) academic grades, g) sex," it defines the data that will be processed in the course of administering driving permits issued in Austria. It does not define, however, *where* (in which database and at which location), nor *how* (in which structure) this data will be stored. However, the *where* and *how* are of utmost importance, when it comes to accessing this data beyond the needs of managing driving permits. This data might be used by a variety of other applications, such as statistical analysis, law enforcement activities, FOI queries, rectification of personal data by the data subject (i.e., the person whom the data is about), and so on.

Fig. 4.3 outlines a few of the uses of this data (FOI requests, interaction with data as part of administrative procedures court-mandated rectification of data, etc.); however, this figure is incomplete and, as a matter of fact, *cannot* be completed. The problem now is that the range and scope of stakeholders which have legitimacy to access this data might change in the near future. Accordingly, the problem is not one that can be solved by specific solutions (e.g., giving law enforcement agencies a technical

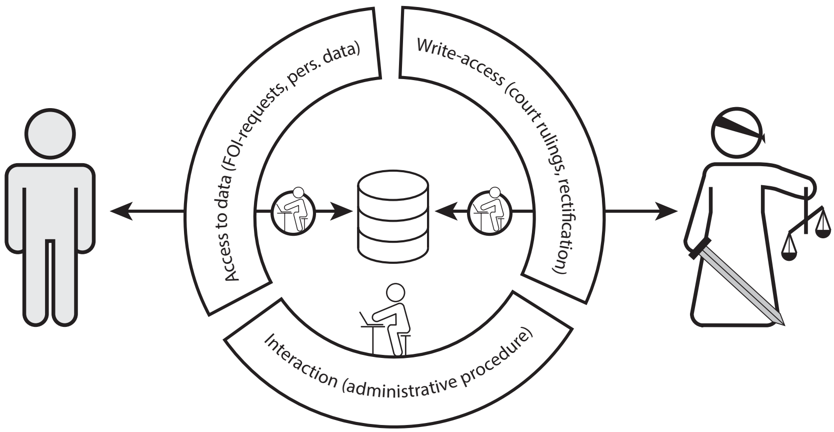

Fig. 4.3 Ubiquitously moderated access to data.

way to access the data), but rather is one that needs a clear approach at a systemic level. This is by far no trivial matter, due to the fact that data traverses a number of different shapes and forms in its journey from the database to the user's screen.

For sake of illustration, let us assume a dataset about a person, like the one shown in Table 4.1. This dataset consists of three attributes—`name`, `dob`, and `sex`, with the corresponding values. In the world of informatics, the individual data entity (here, the attribute) is the lowest form the data is stored in.[11] This data belongs to Bob, who is the data subject, i.e., the individual whom this data is about. According to valid law (cf. Data Protection Working Party, 2007), Bob has the right to learn which data is collected about him. Let us assume then that an online system exists which lets Bob view his data over the Web. What Bob would see on the screen would perhaps look like what is shown in Fig. 4.4.

Now, these are two distinctly different things—one is the data about Bob, as it is stored in a text file on a server somewhere; the other is a visual rendering of Bob's data. There is also another noteworthy layer in between these two. What Bob's Web browser actually receives from the server is text, as shown in Table 4.2. Even though it is likely that the Web client used by Bob might visualize the text from Table 4.2 into what is shown in

[11] If we were to break it down further to the individual logical bits and bytes, or perhaps even further to the individual signals at the level of hardware, we'd enter and cross the domain of computer science. We will deliberately not be addressing this in the scope of this treatise.

Table 4.1 Raw dataset about Bob

```
{
   name = bob,
   dob = 1984-04-01,
   sex = m
}
```

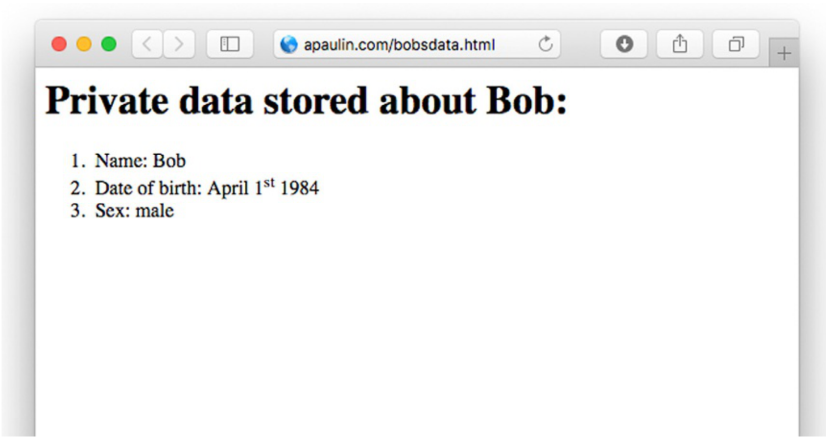

Fig. 4.4 Rendered HTML page in Bob's browser.

Table 4.2 HTTP response containing the HTML page with Bob's data

```
HTTP/1.1 200 OK
Content-Type: text/html

<html>
   <head></head>
   <body>
      <h1>Private data stored about Bob:</h1>
      <ol>
         <li>Name: Bob</li>
         <li>Date of birth: April 1<sup>st</sup> 1984</li>
         <li>Sex: male</li>
      </ol>
   </body>
</html>
```

Fig. 4.4, this is not necessarily always the case. If Bob has impaired vision, for example, he might choose a Web client that reads the responded Web page, rather than displaying it. If he is deaf-blind, he might access his private data through a system that renders the information in braille. We now have three different forms in which the information can be presented—one in which it is stored, one in which it is communicated, and one in which it is consumed. Modern law turns a blind eye to the first two, and only attempts to deal with the last one, that is, where the actual consumer comes in touch with the digested core data.

Now, let us assume that Bob would like to be notified each time the data, which the system stores about him, changes (e.g., a new data entry appears). The interface to access the data is in the form of an HTML page, which has a structure that can easily be read by machines. Bob could then write an application which would open the respective Web page every day and let it extract all the entries inside the first `<ol></ol>` tag from Table 4.2. This is easily achieved—each attribute is sent enclosed within its `<li></li>` tag, and the separator between the name of the attribute and the value of the attribute is a semicolon followed by a space.

This is fine as long as the Web page does not change—but this rarely happens. Agencies are keen to update their Web pages every so often to keep up with the trends and fuel local economy. Fig. 4.5 shows how the Web page might look after such an update. From the perspective of law, the system still gives Bob access to the data stored about him. But from a technical perspective, the update has broken Bob's periodic data checker, which relied on the HTML-level implied *contract* initially offered by the server. Table 4.3 shows the new response: the tags that Bob relied on have disappeared and so has the clear distinction between the attribute name and the attribute value.

The above example demonstrates why the *how* and *where* are important. In the example, interaction occurred at four distinct layers: The first is where the data was stored, that is, the level of a computer file, as shown

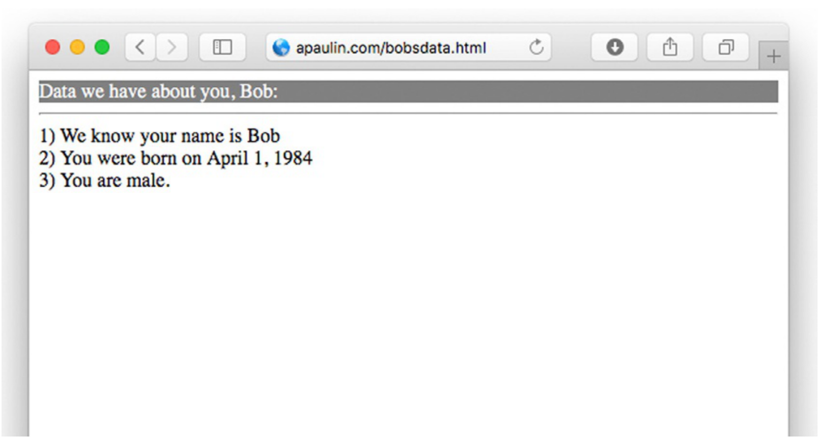

Fig. 4.5 New visualization of Bob's data.

Table 4.3 HTML responded by the new Web page

```
HTTP/1.1 200 OK
Content-Type: text/html

<html>
   <head></head>
   <body>
      <div style="...">Data we have about you, Bob:</div>
      <hr/>
      <div>1) We know your name is Bob</div>
      <div>2) You were born on April 1, 1984</div>
      <div>3) You are male.</div>
   </body>
</html>
```

in Table 4.1; this level can be accessed by having access to the computer (server) on which the file is stored. In this particular case, if one were to play a prank on Bob and change his sex in the file, a simple text editor would be a sufficient enough tool to do so.[12] The next level is the HTTP communication between the server and Bob's Web client—at this level, Bob must know the Web location of the information he seeks. What happens here in reality is that the agencies often change the (technical) locations of particular information—this makes any advanced interaction, such as what Bob did with his application, impossible. The third level is the HTML structure, which Bob aimed to consume with his periodic checker. Again, this level is one at which changes frequently occur. The last level is where the human consumer interacts with the information. This then is the only level which law and law enforcement agencies comprehend and address.

In order to align the law and technology, the law must be properly able to deal with concepts such as the technical *how* and *where*. It is not that this is impossible—this treatise is about exploring how it can be done. Nevertheless, it is an endeavor which requires proper recognition by the stakeholders involved with law (lawmakers, law enforcers, etc.), as well as a full understanding of the subtleties which it encompasses, which as of now does not exist.

[12]The text file used in this demonstration is a fully valid possibility for storing the data—in informatics, this would be called a *flat file*. In reality, however, data would typically be stored in a relational database, or similar, to which data access would be moderated through a data server application.

REFERENCES

Arora, S., 2007. Review and Analysis of Current and Future European e-ID Card Schemes (MSc thesis). Royal Holloway, University of London, London.

Bezeljak, T., 2009. Elektronsko poslovanje v sodnih postopkih zaradi insolventnosti [Electronic operation for insolvency proceedings]. In: Z inteligentnimi sistemi do strateške prednosti. Presented at the Dnevi Slovenske Informatike, Slovensko društvo informatika, Portorož/Ljubljana.

bouncycastle.org, 2015. Supported Curves (ECDSA and ECGOST) [WWW Document]. http://www.bouncycastle.org/wiki/pages/viewpage.action?pageId=362269. (Accessed 20 March 2016).

Bovens, M., Zouridis, S., 2002. From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control. Public Adm. Rev. 62, 174–184. https://doi.org/10.1111/0033-3352.00168.

Burton, M., 2011. A Peace corps for programmers. In: Open Government. O'Reilly Media.

Data Protection Working Party, 2007. Opinion 4/2007 on the Concept of Personal Data. O'Reilly Media, Sebastopol, CA.

Dumortier, J., 2004. Legal status of qualified electronic signatures in Europe. In: Securing Electronic Business Processes. Vieweg Verlag, pp. 281–289.

EU-EC, 2000. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. Official Journal.

Horvat, S., 2011. Centralni register prebivalcev ČG in njegovo upravljanje na podlagi upravnih postopkov [Central Registry of Residency of Montenegro and its management based on administrative proceedings]. In: Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb. Presented at the Dnevi Slovenske Informatike, Slovensko društvo informatika, Portorož/Ljubljana.

Horwitz, M.J., 1982. The history of the public/private distinction. Univ. Pa. Law Rev. 130, 1423–1428. https://doi.org/10.2307/3311976.

Jerovšek, T., 2000. Uvod [Introduction]. In: Zakon o splošnem upravnem postopku z uvodnimi pojasnili Toneta Jerovška in s stvarnim kazalom [General Administrative Procedure Act with an Introduction]. Uradni list RS.

Kolar, D., 2009. E-subvencije in javna naročila [Public Procurement and Subsidies]. In: Z inteligentnimi sistemi do strateške prednosti. Presented at the Dnevi Slovenske Informatike, Slovensko društvo informatika, Portorož/Ljubljana.

Kos, U., Zorman, M., 2009. Ključni faktorji za uspeh IT projekta—Praktične izkušnje ob uspešni prenovi aplikacije CRPsi (Key success factors for IT projects—practical experience from successful renewal of CRPsi application). In: Z inteligentnimi sistemi do strateške prednosti. Presented at the Dnevi Slovenske Informatike, Slovensko društvo informatika, Portorož/Ljubljana.

Lessig, L., 1999. The law of the horse: what Cyberlaw might teach. Harv. Law Rev. 113, 501–549. https://doi.org/10.2307/1342331.

Lessig, L., 2006. Code 2.0. Basic Books, New York.

Mayr, W., 2011. Corruption Scandals in Austria: A Web of Sleaze in Elegant Vienna. Spiegel Online.

Myhr, T., 2005. Regulating a European eID. Porvoo e-ID Group, Reykjavik, Iceland.

Naraks, A., Golob, A., 2009. Informacijska podpora za učinkovito izvajanje nalog Tržnega inšpektorata Republike Slovenije [IT Support for Efficient Execution of Tasks According to Regulation Act of Administrative Procedures]. In: Z inteligentnimi sistemi do strateške prednosti. Presented at the Dnevi Slovenske Informatike, Slovensko društvo informatika, Portorož/Ljubljana.

News.at, 2008. Kinder vom Wiener Stuwerviertel: Baby-Strich gewinnt in Sperrbezirk Überhand [Children of the Viennese Stuwerviertel: Child Prostitution gets out of hand]. NEWS.

Paulin, A., 2012. Status and outlook on electronic identity in Europe: the case of Austria. In: Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and IFIP EPart 2012, Schriftenreihe Informatik. Presented at the IFIP EGOV 2012, Trauner, Kristiansand.

Paulin, A., 2013. Towards self-service government—a study on the computability of legal eligibilities. J. Univ. Comput. Sci. 19, 1761–1791. https://doi.org/10.3217/jucs-019-12-1761.

Paulin, A., Welzer, T., 2013. A universal system for fair non-repudiable certified e-mail without a trusted third party. Comput. Secur. 32, 207–218. https://doi.org/10.1016/j.cose.2012.11.006.

Peled, A., 2014. Traversing Digital Babel: Information, e-Government, and Exchange. Information Policy series. The MIT Press, Cambridge, MA.

Rissanen, T., 2010. Electronic identity in Finland: ID cards vs. bank IDs. Identity Inf. Soc. 3, 175–194. https://doi.org/10.1007/s12394-010-0049-8.

RS-AC, 2011. I U 1589/2010. The Administrative Court of the Republic of Slovenia.

Šinkovec, J., 1998. Odgovornost države za škodo [Responsibility of the State for Damage Caused]. Gospodarski vestnik, Ljubljana.

Toplak, L., 2008. Civilno pravo—splošni del civilnega prava [Civil Law—General Part]. Pravna fakulteta UM, Maribor.

Walter, A., 2011. Das Unbehagen in der Verwaltung: warum der öffentliche Dienst denkende Mitarbeiter braucht [The Apprehension of the Administration—why the Civil Service Requires Staff that Thinks]. Edition Sigma, Berlin.

PART II

Understanding Governance: Fundamental Principles

Part I of this book provided the context in which this treatise is set—it described the trials and tribulations of modernizing public governance by introducing digital technology in the processes of public administration and democratic organizations. It concluded that modern systems of law, which aim to regulate the behavior of individuals and institutions through policies expressed in a natural language, are inadequate to govern technicized systems for public governance. The thus revealed rift between law and technology is a new domain addressed through the remainder of this book.

The chapters in this part provide an overview over the "nuts and bolts" of governance of power relations within a society. To this end, they explore the principles of the emergence of power, that is, the birth of the public apparatus and the fundamental concepts behind the legal relations that make up the *fiat* system of law.

Regarding the birth of power, society, and the public apparatus, many thought experiments aim to depict the emergence of power structures. One such example is Georg Orwell's *Animal Farm*, inspired by the then-contemporary Bolshevik Revolution. Other examples are provided by

Heinrich Popitz' (1976) *Prozesse der Machtbildung*, a treatise that deals with the question of how power emerges and evolves. Another theoretical approach to explain the emergence of governance is the *social contract theory*. Chapter 5 aims to explore this question in further detail.

Once power is stabilized and a society established, a public apparatus can start to evolve based on common rules that govern the relations between stakeholders in the system of power. The core principles that govern the relations within societies and public apparatuses have been explored by Georg Jellinek's *System der subjektiven öffentlichen Rechte*; Wesley N. Hohfeld's analysis of jural relations on the other hand provides insight on the principles of *rights* as elemental relations in societal systems. Both shall be explored in Chapter 6, as they are relevant to the understanding of the background for further exploration of governance informatization. Chapter 6 also sheds light on the vagueness of the term "governance" as used throughout the social sciences, with the aim of finding a definition that is appropriate for transferring societal governance into the domain of technology.

CHAPTER 5

Origins of Power and the Birth of the Public Apparatus

Contents

It is always intriguing to think about how our world came to be. To avoid misunderstandings, it is not the *absolute* beginning of the "universe" that intrigues, but rather what determines a way of life or constitutes the beginning of a culture. The question here about the beginning of our world is thus not a search for an answer to how dinosaurs came into being, but it is rather the search for a *founding myth* of a world (in terms of a civilization/order/culture) that is reminiscent of the creationist myths of religions.

One such myth is the Swiss Rütlischwur, the founding myth of the Old Swiss Confederacy and a core symbol of the modern Swiss national identity. The Rütlischwur (picked up in Schiller's play *Wilhelm Tell*) is the legend of an oath of protection between representatives of three Swiss cantons dated around the 13th–14th century, from which the Swiss *Eidgenossenschaft* (Confederacy) emerged, which survived until the end of the 18th century. Richer in fantasy are founding myths from antiquity, such as the story of

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00005-4

the Trojan prince Aeneas from the *Iliad*, whom Virgil's *Aeneid* made into the founding father of Rome, thus legitimizing the Julio-Claudian dynasty to rule the Roman Empire; or the story of Simurgh, the Persian protector of kings and heroes made famous by Ferdowsi's epic *Shahnameh*; or the figure of the Chinese Long, the dragon composed of features of different animals, symbolizing unity of the nation. The founding myth of the Israelites is found with Israel, brother of Isaac and son of Abraham, whose lineage, so goes the founding myth, is traced straight to Adam, who left the Garden of Eden.

Founding myths of public apparatuses are no less popular in modern time: Socialist Yugoslavia's founding myth was the "Fight for National Liberation,"[1] a powerful and inspiring story of national upheaval against the fascist occupation. In reality, it was more of a struggle of the new bureaucratic class' emergence from the ashes of the old system that was overthrown by the occupying forces (Djilas, 1957). As history teaches, the occupying forces were often not the enemy, but a valuable tool in this pursuit, who willingly traded weapons, information, and ammunition with the domestic revolutionaries (Samardžić, 2006).

The founding myths of the USA—the fight for independence that culminated in the Boston Tea Party, and the later "Liberation of the Slaves" as the just cause of the US civil war—have less virtuous roots than what the myths tell. The Boston Tea Party was less of an act of defiance against British colonialism, but rather a fight of American smugglers of Dutch tea for their turf. When the British aimed to outprice smuggled tea by removing duties on tea from the East Indies, the smugglers responded by destroying all of the tea, dressed up as native Americans (Adams, 2001, pp. 310–311). The US civil war was not about slaves, as schools teach children to believe. Before and during the civil war, political figures such as Lincoln, as well as all three branches of government firmly supported the continuance of the slave system, which was a cornerstone of the South's economy (whereas the cornerstone of the economy in the North was the precarious worker of the industrial system (Adams, 2001, chap. 31)). The civil war was really about the increase in political power of wealthy industrialists from the North in the federal government, which endangered the positions of the plantation owners of the South—there was little compassion for the working classes on either side in this "rich man's war and poor man's fight" (Adams, 2001).

[1]Narodnoosvobodilni boj (NOB).

Founding myths are important for building a sense of unity in a nation. They tell a mythical beginning of a new era, legitimize the break with the past, and lay ideological foundations for the emergence of a new public apparatus. They allow to identify traitors and saints and legitimize demonization of these "traitors," while building statues for these "saints" and entrenching their family members in the new order from the start.

This chapter aims to understand how it all really begins—i.e., beyond the narratives of founding myths. Section 5.1 explores the microorigins of power and its perpetuation into systems of governance; Section 5.2 embarks on a virtual journey through an imagined society from the beginning of governance to the rise and continued evolution of a public apparatus; and Section 5.3 reflects on the mythos of the *social contract*, a founding myth popular in political science which aims to trace the basis of legitimacy of governance systems.

5.1 POPITZ ON THE ORIGINS OF POWER

Heinrich Popitz' 1968 *Prozesse der Machtbildung* is a collection of three thought experiments that aim to explore how power is established, and, hence, how governance as such emerges from a blank slate situation. His work contributes to the understanding of how power structures develop and evolve into gradually more elaborate systems of governance. His first thought experiment takes place on a cruise ship, where organization emerges around the control of deck chairs. The second experiment is placed in a prison camp, where a group of inmates build a stove and develop it into a self-perpetuating system of power that keeps this stove as their monopoly. The third experiment is set in a boys' home in which one group of boys systematically oppress the others in order to establish and perpetuate their position of privilege.

Understanding how power emerges and perpetuates itself is of relevance to the present treatise for two reasons: First, it explains why it is *not* possible to informatize governance from scratch; i.e., technology as such cannot cultivate a society without other sources of motivation—for this same reason an ideology by itself provides no tool to plant and cultivate a civilization from scratch. The second lesson to learn from Popitz' explorations is that a blank slate may well be found in niches along existing structures and levels of power and governance. The rift between written law and the new possibilities brought about by cyberspace is this blank slate, on top of which new power structures can emerge with the goal to informatize governance.

Following are short summaries of the examples given by Popitz. For a deeper discussion on the topic, Popitz' original text is highly recommended.

5.1.1 First Case: The Deck Chairs

A cruise ship sails along the Mediterranean Sea, docking at various harbors along its route. At each harbor some passengers leave and others enter. On the deck of the ship are deck chairs, which the passengers can make use of. The number of passengers significantly outnumbers the number of the deck chairs; however, since the chairs are not constantly in use, there are always a few chairs left unoccupied for whoever may want to use them. Once a passenger leaves a chair, the chair becomes free for use by others. The community does not recognize the reservation of a chair, and if someone puts a towel on the chair to reserve it, another passenger will simply remove it to use the chair themselves. The *culture* that the chairs must not be reserved becomes well established to the benefit of all.

A batch of new passengers arrive at one of the harbors and start occupying the desk chairs for themselves. A system of solidarity establishes itself among this group of *possessors*, to protect their chairs and bring more and more under their control. If a *nonpossessor* approaches a vacant chair, the other *also possessors* start shouting at him and threatening him. The system evolves ad hoc from the solidarity among neighbors who thus defend their mutual interest: when a *possessor* leaves his chair, he'll ask his neighbor to help him keep his chair, which the latter will do, since they will expect the same favor in return.

However, this system still requires that a significant number of the *possessors* are constantly alert to defend the chairs from *nonpossessors*, plus the possessors themselves must engage in the unpleasant act of shouting at occasional intruders. Out of opportunity to reduce the burden on the possessor group itself, the protection of the deck chairs is soon outsourced to some of the *nonpossessors*, who in return are allowed to temporarily use the chairs. Thus, the society becomes divided into three classes: the possessor elite, the working class consisting of guards and other service providing nonpossessors, and the other nonpossessors, who have no access to the chairs. The division of the society results in a self-sustaining hierarchy, in which the working class continues to support the elite.

The society here developed from an ur-anarchy, in which everyone had equal access to the shared resources for the common benefit of all, into a governed society which protected the mutual benefits of the minority that took part in the scheme. This brings up the question of how an aggressive minority could bring the shared resources under their sole control, even though this was clearly against the common interest of an overwhelming majority. The reason is simple: The minority had managed to *organize* themselves into defending the mutual interest of each individual *also possessor*. The majority on the other hand had no *mutual* interest available, but rather merely the *common* interest of returning to the previous state of anarchy. This *common* interest, however, did not bear the potential to organize into a coordinated group that would put the existing system out of power. If an opposition could organize itself and manage to liberate the desk chairs, this would inevitably position this new group to bring the chairs under their control, and thus only exchange one hierarchy for another, i.e., one system of governance for another.

5.1.2 Second Case: The Prison Camp

Popitz' second example is set in a prison camp, in which prisoners of war are kept under highly primitive conditions. Facilities are nonexistent, making fire is forbidden, and the food is brought in raw to the prison camp. A random group of inmates band together, each of whom has a specialization that enables this team to build a stove in secrecy and protect it from any outsiders.

At first, the group engages in trading, offering their services in exchange for goods. Soon the demand for the stove becomes much higher than what they can supply, so access to the stove becomes a privilege which is granted as a special form of mercy and reward by the group (yet still for a high price). The priority of the group becomes the maintenance of their stove monopoly in the prison camp; hence, their aim is to prevent any other group from establishing their own stove, i.e., to prevent competition. With control over the stove, they build a loyal class of supporters, who help them to defend their monopoly. This network of supporters ensures that no other group is able to build a stove for themselves. They ensure this by deploying techniques of sabotage and subversion.

To sustain their monopoly, the center of power deploys tactics of *divide and conquer*. Gradually, a division in the society is accomplished—there are three layers circled around the elite group of power: The first layer is the class of supporters, which provide services such as defense, espionage, or subversion in exchange for limited access to the stove. The second layer is the neutral majority, who abstain from any action that could get them in trouble if messing with the business of the system. The third layer is the oppressed minority, which the system of power can victimize and prosecute at will. In this function, this victimized minority is a vital part of the system of power. In order to spread and sustain, the system constantly chooses new groups of victims and acts against them. By this, the group of neutral observers slowly reduces, as the members of society are either active members of the system or its passive victims.

5.1.3 Third Case: The Redistribution System

Popitz' third case is placed in a boys' home, in which a system of power has matured to a stage where it has become a redistribution system, and provides rents to its stakeholders. From the 13 boys in the home, four boys form a center of power, and three other boys are held by this group as a task force. The six other boys are subjected to a system of exploitation. One of the leaders is the "boss," who can provide the final ruling if necessary.

For breakfast, each boy receives two slices of bread, from which the exploited six boys are forced to give one slice to the system of power—this affords the system a daily income of six extra slices of bread. The task force exacts these contributions from the exploited boys and delivers five pieces to the center of power. From these five slices, the boss receives two pieces, and the other three one each. The sixth slice is divided between the three members of the task force, resulting in an income of one-third slice of bread each. If any of the boys do not comply with the commands from the circle of power, the system delivers some harsh punishment, whereby the entire group of boys is made to actively participate. Thus, a neutral group of observers, which had existed in both the above-described cases, has vanished in this case.

In this particular situation, the central circle of power created two levels of exploitation: the lowest layer was to give away half of their daily ration, while the middle layer has to provide their services in exchange for some minor share. The recipe for sustaining power here was to maintain a balance between the two oppressed groups. The center of power achieves this by exploiting the weaknesses of the others. The weakness of the lowest group was that they were in constant danger of losing even more than what they already had; if a boy from this group dared to rebel against the system, he might risk not only going to bed hungry, but also being beaten up. The weakness of the task force was that they could easily be replaced. If a boy from the task force was to rebel, he would risk falling even lower in the hierarchy, as there were four others who could easily (and eagerly) take his place. It is this constant fear of losing the status granted by the system which allows the system to perpetuate itself—paradoxically, the system is driven by the motivation of the oppressed, who fear losing their bad position for an even worse one.

5.1.4 Conclusion

Popitz' examples provide insight not only into the emergence of power, but ultimately also into the *perpetuation* of power. This very perpetuation of a power culture, which evolves from the realization of a random opportunity, requires a stratification of society—the creation of social layers protects the inner circle of power. The conclusion is that in order to establish a system that can sustainably provide some social functions to the society, a sufficient supportive ecosystem must be cultivated—in the above-described cases, these were the guards, the henchmen, the minions, and the task force. It is in the interest of those in this supportive ecosystem to protect and sustain the system that is built around the circle of power. One major point to note is that once a system becomes sustainable, it is near impossible to destroy or replace it.

The combination of a power vacuum and limited resources in the case of the Web has also encouraged the emergence of new systems of power within the cyberspace. Organizations such as the *Internet Corporation for Assigned Names and Numbers* (ICANN), which governs the global domain names (it leases the Internet addresses ending in .com, .org, etc.), or the *World Wide Web Consortium* (W3C), which standardizes the structure of Web pages (HTML) and other Web formats/technologies, etc., became the de facto authorities within the digital dimension in a manner similar to the power structures described by Popitz.

While systems of power aim for self-perpetuation, this does not necessarily prevent competing systems from emerging. Established systems of power might also die out on their own, if, for example, the value of the controlled central resource becomes insignificant. A rival system's main challenge is then how to subvert the established system of power by offering a more promising ecosystem for individuals to switch into.

5.2 GEDANKENEXPERIMENT "RIVER SOCIETY": RISE AND DECLINE OF A PUBLIC APPARATUS

Popitz' thought experiments on the origins of power deliberately stop at the stage of perpetuation of power. He consciously omits the further phases that allow systems of power to evolve from a primitive hierarchy to a public apparatus. It is the maturation of a governance system to a complex public apparatus which offers opportunities for more advanced systems to evolve, such as systems of politics and strongly structured administration. That in turn opens up opportunities for technicizing the public apparatus. The following Gedankenexperiment considers what further evolution of power structures might look like, taking inspiration from the European 20th century transition to a welfare society.

On a river which divides two settlements, ferryman Franck provides his service to cross the river. The service is a private business—Franck's father built the ferryboat decades ago, and Franck maintains it, using the income generated from this business to provide for his family. Franck inherited this trade from his father, Franck's son will succeed him, and so on. Franck is honest and modest, and his business is respected for the social function it provides to the communities on both sides of the river, so they happily pay the fair fee for the services Franck provides. There are months or even years when business is bad, due to low trade. In such periods, Franck lives off his savings which he had accumulated from the more profitable times. Then again, there are periods when trade is so high that Franck is barely able to serve the river crossings; at times like these, Franck thinks about expanding his fleet and hiring people to help him.

The blossoming trade relations between the settlements during the years helped Franck to accumulate wealth. The economic prosperity, however, lured in foreigners to invest in the economy, and so a company specialized in constructing bridges, *Bridge Ltd.*, soon built a bridge over the river. Bridge Ltd. charges a fee for crossing the bridge that is slightly higher than what Franck charges, but then again, their service is much more convenient: no waiting for the ferry, no restrictions with regard to weight, and one can also cross the river by night.

5.2.1 Stage I: Rise of Government

The bridge quickly puts Franck out of business. As soon as Bridge Ltd. finds themselves in a monopolistic position, they begin to steadily raise the prices for their service. Year after year, the prices are "adapted to inflation"—the prices for elementary goods and services are rising (as rumor has it, due to increasing costs of transportation). To increase their profit margins, Bridge Ltd. abandons proper care for the aging bridge, and soon damages to the pavement become a nuisance.

Dissatisfaction with Bridge Ltd. and the rising prices grow, and seizing the opportunity of the moment, *Paul, the politician*, sparks a movement against the "greedy" Bridge Ltd., calling for a "nationalization" of the bridge. The bridge, in Paul's narrative, is a matter of public importance—the economy of the two settlements relies crucially on the bridge. It is only just and in the interest of everyone, according to Paul, if the bridge was liberated from the claws of the greedy foreign capitalists. Besides, and Paul really cannot stress this too much, the bridge was built by the sweat and pain of the locals, not the dirty money of the foreigners!

In the fight for the just cause, Paul argues that everybody must make a small contribution; hence, Paul's boys start levying taxes to support the movement. The taxes are collected so that Paul can provide for his boys, who risk their lives and good fortune for the noble fight against the greedy oppressors. Paul's promise that once the bridge is liberated, crossing it will become free for all, is hard to object to, and besides, nobody wants to be seen as a traitor to this glorious liberation movement (many have even disappeared under mysterious circumstances already); therefore, everybody willingly pays their contribution.

Paul's movement easily drives Bridge Ltd. out of town, and Paul, being a man of honor, keeps his word and makes crossing the bridge free of charge. The newly gained liberty is a happy moment for the river society and introduces a period of sudden growth in the society's purchase power: with the elimination of the fees for crossing the bridge, goods and services have become more affordable than ever, even though the trader's profit margins have never been higher.

In this moment of economic prosperity, nobody cares that Paul's tax collection continues. And Paul, the society's new hero, is applauded when he declares that from now on, he and his boys will take the hard responsibility of governing and protecting the bridge as a *common good*, naturally, for the sole benefit of the community, whose right to cross the bridge "for free" shall be enshrined forever.

5.2.2 Stage II: Birth of the Public Domain

As time passes, the bridge requires more and more repairs. Aside from this, new investments are planned to enhance the functionality of the bridge, such as better illumination, a quieter road pavement, and the like. Since it is in the common interest that the bridge remains in good shape, Paul sees himself forced to raise taxes to cater to the new expenses. Since all of this government business is getting too much for Paul, he entrusts the maintenance of the bridge to his brother, who in turn commissions his brother-in-law to carry out the overdue maintenance works.

But *Carl, the contractor*, is not amused by Paul's clan getting all the government jobs—it is taxpayer's money after all. Carl was among the hard-working laborers who built the bridge in the first place and one of the strongest supporters of the liberation of the bridge. Carl is convinced that the spending of taxpayer's money must be transparent and that those in positions of power must be held accountable for their decisions and actions. Carl also accuses Paul's clan of spending money on luxuries (like the new low-noise road surface), rather than on "things that matter."

Franck, who still remembers his father's flourishing ferryboat business, shares Carl's criticism; however, Franck's view is that the bridge should be torn down (its maintenance is too expensive after all), to make things as they were in the good old days: "away with the bridge and lower taxes!," he demands.

Having Paul as their common enemy, Carl and Franck call for a platform for deliberations on public matters, which will decide on public policies, public spending, and other matters of communal concern. They fiercely demand an end to Paul's absolute monarchy and demand a parliament that will decide instead of Paul alone.

5.2.3 Stage III: Rise of the Bureaucracy Caste

Instead of Paul alone, it is now the triad Carl, Franck, and Paul who decide together how the taxpayer's money is distributed. The bridge remains in its place, but a separate bureau has been established, headed by Carl, which administers the maintenance of the bridge. Paul is no longer in charge of the bridge, but considering his vast insight into the affairs, he is a valuable and respected member of parliament. His former role of chief tax collector has now been embodied into the internal revenue office, in which Paul and his boys continue business as usual. Franck has been appointed president of the parliament, but his fight for lowering the taxes has been stifled by the real scale of the occurring expenses. Besides, as he now gets a good income from his new function, he has lost his ambition to return to the harsh labor and tediousness of operating the ferry.

Taxes are raised a little to allow for further inclusion of public deliberation on public matters. Indeed, numerous new issues have emerged, which previously seem to have been overlooked. For example, there are stringent security implications due to the expanding population of crocodiles in the river, which also strongly affects the fishing economy. Furthermore, rumors of acts of indecency going on in the night under the bridge have begun to circulate. To provide security and protect public morals, the parliament ventures into lengthy debates, in the search for a solution.

Tom, the teacher, and *Hank, the healer*, strongly disagree that all of the taxpayer's money should be spent on bridge-related issues. The money would be better spent on public education and public health. A healthy and well-educated society, they argue, would bring more benefit to the economy of the river society than all the nonsense investments in the infrastructure around the bridge. *Sam, the scientist*, and *Pierre, the painter*, couldn't agree more, and so they join the call for a thorough reform of government.

5.2.4 Stage IV: Rise of the Public Apparatus

Ann, the civil-society activist, is also dissatisfied with the evolution of society: All decisions are made behind closed doors by Carl, Franck, and Paul, and only this small elite has access to information and resources. Ann demands "true democracy," fair elections, access to public sector information, and more participation in political decision-making, which must be open to all. The public, after all, must have the right to be heard, the right to participate, and the right to know where their money goes. The *Intelligentsia* (Tom, the teacher, Hank, the healer, Sam, the scientist, and Pierre, the painter) join Ann in her fight for an open, more inclusive, and "better" society.

Carl, Franck, and Paul give in to the public pressure that has built up and introduce popular elections, open to all. They have little to fear: the internal revenue service is firmly in the hand of Paul and his boys; Carl is in charge of the bridge maintenance bureau. To secure Franck, a new bureau has been created that organizes the elections, registers the political parties and voters, and is responsible for any matters related to the political processes.

On election day, Ann and the Intelligentsia firmly win, pushing Carl, Franck, and Paul out of the parliament. To fulfill the promises given to the public, Tom and Sam get a public education bureau, Hank one for public health care, and Pierre embarks on a mission to foster the advancement of fine arts.

Under Ann's new government, the economy thrives; arts, science, and technology flourish; and given the splendid economic indicators, few consider to object that a loan is taken up to build a new bridge. As the public apparatus now provides so much more, the taxes are raised further, but nevertheless—according to Sam's studies—the happiness index of the people is the highest ever recorded.

5.2.5 Stage V: Recession and Collapse

The increasing taxes lead to increased prices for everyday goods and services, while the profit margins decline to accommodate for the lower purchasing power. More and more businesses become unsustainable and close down, some after many generations of existence. Unemployment becomes a severe issue and a heated political debate now centers on how to deal with the social situation. Due to the social challenges, there is less income for the society's communal budget. Keeping up the various functions of the public apparatus, while repaying the loan for the new bridge, becomes impossible.

In the next elections, Paul's radical plans convince the populace and in order to save what can be saved, Paul introduces stringent austerity measures and cuts funding across all domains, cutting down on "luxuries" like science, health care, and arts.

Meanwhile, the others have become strongly accustomed to their lavish lives in the bubble of the public apparatus. Paul's cutting down of their domains is an unexpected inconvenience, and thus they begin to plot against Paul. They're determined to remove him from his position of power—by force, if necessary.

5.2.6 Summary

The above-described evolution of a fictional society culminated in a public apparatus, in which taxes were levied, a deliberation platform (the parliament) had been erected for public-domain governance, and principles such as transparency and accountability became relevant. Although this Gedankenexperiment is based on a highly simplified account of a real-world public apparatus, it nevertheless can serve as a workable model in attempting to understand the many challenges and implications of the dynamics of public governance. As such, it may serve in testing ideas to transform public governance, as the one presented in this treatise.

5.3 SOCIAL CONTRACT THEORY: DOES IT STAND THE TEST?

The fascination for the origins of structures and systems of power is an everlasting one. The interest in this topic is twofold: On the one side, it is a fascination for one's own fate within the social hierarchy, which makes one wonder how a minority is able to control the majority. On the other side, it is a question of how structures and systems of power can justify their legitimacy with regard to the role they play. A popular notion is that systems of power are *needed*, and that they exist out of the necessity for their existence. This notion is further supported by the *social contract theory*, a secular counterpart to the hypothesis of the divine right to power, driven by the works of Hobbes (1651), Locke (1689), and Rousseau (1762), to name but a few.

Thus, political philosophy teaches us that the beginning of society is the *social contract*—an implicit ur-agreement among the members of a community, by which the community entrusts some system of power with governance. In exchange for rights, which the system of power grants and protects, society gives up some of its liberties. Even today, some scholars believe that "thousands of years ago, human ancestors had no governments and lived in what is said to be the primitive state of human existence, [… where …] life was solitary, poor, nasty, brutish, short, and mainly characterized by self-interest and that there was need for a power […]" (Aham-Anyanwu and Honglei, 2017), which emerged based on the social contract—"an agreement made thousands of years ago by primitive human ancestors to surrender their natural liberties in exchange for social order" (Aham-Anyanwu and Honglei, 2017).

This theory stems from the European enlightenment period, which is marked by political struggle against the power of the Roman Catholic Church and goes hand in hand with a sharp rise of the public apparatus of modern states. Taking the *social contract theory* at face value would be rather unwise. Considering the examples from Sections 5.1 and 5.2, one cannot easily find an *ur-contract* that grants power to the system. Instead, an intrinsic motivation drives those in power to brutally pave their own way by suppressing the liberty of the community. This inner circle of power did not actually make a deal with the community that could be expressed in a contract. In these stories, systems of power were not needed, wanted, nor called for, yet they emerged because they were able to organize themselves and seize their opportunity.

As such, the social contract is not more than a sociological model, a tool that can help to imagine a fictional birth of society, or to legitimize the existence of authority without resolving to God. That is not to say that this model is of no use in the context of technicizing governance. It provides a useful tool in analyzing the governed community as a system that consists of three elements, namely the abstract sovereign, a system of rights which this sovereign grants and defends, and the sovereign's subjects, who lose their liberty in exchange for the system of rights.

The model of the social contract can be applied in already matured power systems. For example, explicit contracts/agreements can establish umbrella organizations that provide governance to their member organizations, supranational organizations that govern relations between nation states, arbitration courts, etc. Implicit social contracts on the other hand can emerge in new domains which lack governance. Such formation of implicit *social contracts* can be observed in the maturation stage of the Web, in which standardization consortia sprang up to govern the infrastructure of cyberspace. But then again, it was not the *need* for governance, but plain and simple *opportunity* that gave birth to these new organizations.

REFERENCES

Adams, C., 2001. For Good and Evil: The Impact of Taxes on the Course of Civilization, second ed. Madison Books, Lanham, MD.
Aham-Anyanwu, N., Honglei, L., 2017. E-state: realistic or utopian? Inter. J. Public Adm. Digital Age 4, 21.
Djilas, M., 1957. The New Class—An Analysis of the Communist System. Thames & Hudson, London.
Hobbes, T., 1651. Leviathan.
Locke, J., 1689. Two Treatises of Government. Awnsham Churchill.
Rousseau, J.-J., 1762. Du Contrat Social [The Social Contract].
Samardžić, M., 2006. Saradnja partizana sa Nemcima, ustašama i Albancima [Cooperation of the Partisans with Germans, Ustaša, and Albanians]. Pogledi, Kragujevac.

CHAPTER 6

Understanding Jural Relations and Governance

Contents

Georg Jellinek's fin-de-siècle theory on the state as a system of subjective public rights and Wesley N. Hohfeld's early 20th century theory on the fundamental jural relations are two of the major theories that explain the "nuts and bolts" of the legal systems. In order to understand how to technicize governance, as this treatise aims to do, it is necessary to understand how systems of law work. Accordingly, this chapter provides a working understanding of both theories in order to establish a sound transdisciplinary theoretical background.

When dealing with deeply interdisciplinary matters, as shall be done in this chapter, one must keep in mind that we are dealing with intellectual perspectives of scholars from multiple generations. These scholars lived in times of varying degrees of access to technology, and from the works we'll be following, did not have the chance to experience cyberspace that modern ICT created throughout the past couple of decades. Their input thus must be understood for what it is: deep knowledge gained from a mono-disciplinary insight, presented to a mono-disciplinary audience. When transferring this knowledge into the realm of technical sciences, as is done in the present treatise, a projection to the rules and principles of the target domain must be performed, so as to avoid any pitfalls posed by reality.

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00006-6

One thing we can assert about society is that it is a dynamic system of subjects who are subjected to a myriad of bureaus that inhabit the public apparatus. The society and the public apparatus behave chaotically in the sense that it is impossible to predict their state in the future, even if exact and complete knowledge was known of the past society. This statement does not ignore the existence of economic, sociological, or anthropological theories, which aim to predict the future state of their observed system. But compared to the level of precision that is inherent to natural sciences or technology, in which predictions of future states of systems enabled reasonably precise weather forecasts, missile-defense systems, etc., the ability of soft sciences to predict the future course of there-observed systems is relatively insignificant. Thus, it would be outright absurd to predict the exact legal regulations valid in the city of Vienna 20 years from now, even if all the minds of all the people in the world were captured and their ideas and sentiments analyzed. It simply is not possible to predict the state of society in the future.

But there are underlying principles—natural laws, so to speak—that govern how the (political) society/public apparatus functions beneath the surface. One such core principle is the egocentricity and self-care attitude of humans, as reflected by the public choice theory (Downs, 1967). But this attitude is not something one could structure and technicize, much like one cannot structure and technicize dreams, ideas, or physiological urges. What can be structured and technicized, as shall be explored in Section 6.3.2, are the formalized relations, based on which a public domain is governed.

Given the broad trans-disciplinary character of the issues at stake, the vocabulary as offered by the *social contract theory* shall be taken as a trans-disciplinary juncture. This theory teaches us that society is *a system* that consists of (i) *subjects*, which are governed by (ii) *the sovereign* and (iii) *rights*, which the sovereign, as the origin of all rights, grants to its subjects. This part of the theory is perfectly usable for a technical exploration, as it provides a clear separation of concerns: subjects are the people acting within the domain of the sovereign; the sovereign is a logical entity (e.g., a privileged subject, a set of subjects, or an abstract entity altogether, such as "the law"); the rights, then, are granted by the sovereign to its subjects in accordance with an underlying *fiat* system. This *subject-rights-sovereign* model can be applied to each stage of the *river society* (Section 5.2), without making the assumption that a specific underlying system of written law exists, nor rejecting such.

Modern legal theory uses this knowledge from *social contract theory* to model the relations among the members of a society (Boyle, 1993; Jellinek, 1905, p. 32). In jurisprudence, every subject (natural person, company, club, state, etc.) has the so-called *legal subjectivity*, which means that they can have (legal) rights and be subjected to duties (Cerar, 1996, n. 4). Legal subjectivity is granted by the sovereign to its subjects (people or associations of people (Jellinek, 1905, p. 77)) in the form of *legal status*—an attribute/characteristic that allows subjects to obtain rights (Jellinek, 1905, pp. 78–79). *Rights* (as well as all jural relations) in mainstream legal theory, as defined by Hohfeld, are relations between exactly two subjects (Hohfeld, 1920; Lazarev, 2005; Smith, 2011), in which one direction of such a relation defines the *entitlement* to claim protection by the sovereign (Jellinek, 1905, p. 77), while the other defines the corresponding duty (cf. Vodinelić 1976 in: Cerar, 1996, p. 10).

In modern developed countries, one of the several[1] sovereigns is the democratic state, which acts through its institutions (Kersten, 2000, pp. 253–261). The sovereign is the source and protector of most of the jural relations, as well as the origin of citizenship and other jural statuses. The management of those jural statuses and the protection of their integrity is a core priority of the sovereign—it is an essential task of *governance*. Based on these premises, one may think of society as a network of subjects who are bound to each other through Hohfeldian jural relations—the so-called *bundles of sticks* or *bundles of rights* (Johnson, 2007; Smith, 2004, n. 30). The crucial function of governance thus becomes the protection of the integrity of this *network of jural relations*.

In Section 6.1, we further discuss Jellinek's system of subjective public rights, and Hohfeld's analysis of jural relations in Section 6.2. Section 6.3 discusses the term "governance" by outlining its many definitions as used in political science, and trying to elaborate on a definition for the scope of this treatise.

6.1 JELLINEK'S SYSTEM OF SUBJECTIVE PUBLIC RIGHTS

Georg Jellinek's *System der subjektiven öffentlichen Rechte*[2] is a classic in jurisprudence. While it is not free from criticism, it remains a valid and influential work over a century after its initial publication (Kersten, 2011, p. 43). In this work, Jellinek founds the *Statuslehre*, a school of thought that abstracts

[1]There are situations in which one would be subjected to another sovereign, for example, with consular staff, who are subjected to an external sovereignty.
[2]System of Subjective Jural Rights.

the entire relation between individuals and the state to a *jural status*, which varies in quality and extent over time. This jural status falls into four distinct categories, which define how a subject can behave in formally governed interactions. More specifically, this jural status defines which *subjective rights* a subject can obtain and possess. Each subjective right requires the existence of a legal system that creates it, recognizes it, and protects it to some extent.

Within the legal system, only abstractions (virtualizations) of natural entities exist. A natural entity is a car, for example. If this car is sold, in the eyes of the law, what is transferred is the associated property rights—e.g., the right to possess the car. The physical handover of the car, however, happens outside of the legal system. If the seller refuses to hand over the car, the buyer has the right to call upon the authorities for the protection of his legal rights. Legal relations such as these, e.g., the relation between the seller and the buyer of the car, between the buyer and the authorities, and between the authorities and the seller, then form the system of subjective public rights. What constitutes these relations are then *rights*, such as property, possession, right of lien, purchase, lease, marriage, inheritance, to name but a few. In order to abstract/virtualize natural entities, jurisprudence refuses to ask what something *is*, but instead asks how something *can be thought of* so that it can be managed within law (Jellinek, 1892, p. 20ff.).

6.1.1 Jural Entities, Jural Subjectivity, Jural Behavior

Jural entities are concepts which can be recognized by humans as something that can be identified and controlled in some way and be subjected to law. Jural entities can be coherent actions such as hikes, train rides, or work; usable things such as domestic animals or cars; geographic continuances like highways, lakes, or rivers; jural *Zweckeinheiten* (purpose-dedicated units) such as clubs and companies; or repeating events such as holidays and anniversaries; etc. These entities are context dependent, and thus one and the same entity considered in different contexts can be something different.

For the jural interaction with jural entities, jural subjectivity is required. Jural *subjectivity* (*Persönlichkeit*) is a relation of one subject to another, and to the legal system (*Rechtsordnung*) as such. Subjectivity is the ability of a legal entity to *have* rights, which can only be created by law. Jellinek argues that there is only jural subjectivity and no natural subjectivity as such, and hence natural persons must acquire jural subjectivity as a precondition to have rights. (For example, Jellinek argues that slaves were natural persons who existed only as *objects* of trade and use, but had no jural subjectivity and thus were not *subjects* before law.) The state has *subjectivity*, as this is a logical necessity to be a partner in jural relations toward its own subjects, as well as other states.

Jellinek distinguishes between the *legally relevant* and *legally indifferent* behavior of subjects. The legally indifferent behavior, for example, is *not-regulated* behavior, such as taking a walk or sleeping (as long as these are not regulated). The *legally relevant* behavior can then be either *legally allowed* (das *rechtliche Dürfen*) or *legally not allowed* (das *rechtliche Nicht-Dürfen*). If a behavior is legally not allowed ("one must not"), i.e., prohibited, this does not prevent somebody from still factually behaving in such a prohibited way.

Jellinek argues that in the case of not-allowed legally *indifferent* legal actions, the respective action is not *unpermitted*, but rather (legally) *undoable*. Thus, he argues, it is not the case that jural subjects could not agree on a *legally not-allowed* contract for the reason that it would not be permitted, but rather that they cannot achieve a valid contract, as it is undoable. Law does not prevent subjects from making an *undoable* agreement, but rather denies its protection and enforcement, as such juridical action is *legally indifferent/irrelevant*—it does not exist before law. Thus, claims for enforcement of a contract about things that have been declared *extra commercium* have to be denied by the court.[3] Not-allowed legally *relevant* actions on the other hand are *disallowed*, and the legal system provides means in order to prevent them—through, e.g., systems of law enforcement agencies.

The entirety of *legally relevant allowed behavior* (Jellinek calls this *legally possible* behavior[4]) does, as he argues, constitute the jural personality, i.e., subjectivity (Jellinek, 1905, p. 55). This means, in essence, that the amount of individual *legally possible behavior* determines the jural subject's situation within the state and the rights and privileges it can acquire and request protection for in case needed. Considering the jural subjectivity being a relation between the subject and the state, one can understand subjectivity as a quality that varies in size through the course of the subjects' jural existence.

6.1.2 Four Categories of Jural Subjectivity

Jural subjectivity comes with a *jural status*, which is a variable that spans four categories—*passive, negative, positive,* and *active*. It is the jural status which enables subjects to undertake *legally relevant action* within the society.

[3] The case described in Section 1.3.5—i.e., the selling of land under restitution—is a case of an *undoable* contract. It was *undoable* since law explicitly declared it as a thing outside of law.

[4] "Die rechtlich relevanten von der Rechtsordnung gewährten Fähigkeiten bilden *in ihrer Gesamtheit* das rechtliche Können" (Jellinek, 1905, p. 51, emphasis added).

The four categories of the legal status, Jellinek argues, are acquired incrementally—the most basic status is the *passive* and the most powerful the *active* status. Each status includes within it the features of the lower statuses. The four categories are defined as follows[5]:

- The *passive* status (*status subiectionis*) describes the duties which the subjugated jural subject has toward the sovereign—e.g., paying taxes, obeying traffic regulations, respecting public authorities.
- The *negative* status (*status libertatis*) is the freedom of subjects to pursue their interests outside of the constraints of the sovereign's restrictions.
- The *positive* status (*status civitatis*) enables subjects to lay claims to recognition and protection of their *legally relevant allowed behavior* from trespassing and nuisances of others, as well as to claim recognition and protection of their *negative* status (Jellinek, 1905, p. 105).
- The *active* status (*status activus*) entitles subjects to participate as part of the state, to exercise political rights, assume public office, and gives them power to act on behalf of the state. For example, the power possessed by judges, administrative officials, and the police.

On the one hand, the sovereign's role is to protect *legally relevant allowed actions*. It does so by entitling jural subjects to demand *legally allowed actions* from subjects who have an *active* jural status. One such example could be to call upon law enforcement agencies to punish trespassing. On the other hand, the sovereign's function is to take measures in prosecuting *legally relevant disallowed behavior*. Any activity of the state is restricted to dealing with *legally relevant* behavior, as *legally irrelevant* behavior is identical to the freedom of subjects, which does not concern the state.

Freedom (the *negative* status) can be restricted, either on a general level, such as when the state restricts access to resources or professions through concessions, or on an individual level, when, for example, a subject is imprisoned. Jellinek argues that granting a concession does not increase the subject's natural freedom of action, but rather removes the respective general prohibition (to exercise the particular behavior). Thus, he argues, concessions for professions such as lawyers, physicians, hunters, and professors do not increase their natural freedom, but reduce *legally not-allowed actions* for the concessioners.

It is the *positive* status which allows subjects to claim recognition of their subjective rights from the sovereign, as well as to claim their protection.

[5]For a comprehensive discussion on the jural statuses, see Jellinek, 1982, chaps. VIII-X. Jellinek omits a deeper discussion on the *passive* status, but instead focuses on the other three which deal with the empowerment of the subject in relation to the state.

The state, through its *jurally active* subjects, recognizes these claims and undertakes actions to protect the subjective rights of subjects. Jellinek argues that the *active* jural status promotes the individual to a level of a state body, though the amount of *legally allowed* behavior, which the subject enjoys in such a role, does not influence the individual's subjective rights; instead, this behavior represents the competences of the state body itself. For example, a judge will exercise the *legally allowed* behavior of their role, such as sentencing others to prison time, only within the scope of their official authority, and are not able to behave as such in their private time.

In order to be able to claim the active status or to increase its competences, the individual must have an active qualification, such as being a member of a specific group. Such membership could be citizenship that entitles individuals to participate in elections, membership in the aristocracy which entitles one to attain rank in the state bureaucracy of traditional empires, or membership in the ruling family clan that enables individuals to claim the crown in monarchies. Modern party politics also usually prevent nonmembers of political parties from assuming public offices of higher ranks.

6.1.3 Technicizable Levers Exposed by Jellinek's Theory

Jellinek's *Statuslehre*, as summarized herein, provides a framework that structures the jural system into a system of core jural actors, namely jural subjects with dynamic jural statuses. Such abstraction of society allows the modeling of virtually unlimited political forms of state or snapshots of public apparatuses—this is of great value when engineering systems to technicize governance.

Concepts such as *government, state,* and *citizenship* become abstracted to systems of jural subjects of varying jural statuses that allow them to exercise particular juridically relevant behavior. Such systems can then, in their entirety, be perceived as functioning governed communities. Ultimately, the system "state" consists of jural subjects (individuals and associations with a recognized jural status), who interact with one another in the jural sphere of a society by manipulating the jural relations between themselves to reflect each other's rights and duties. This permanently evolving ocean of elementary jural relations is what makes up governed human societies ever since.

The abstract concept of the jural status implies the ability to design and modify one's role within the society. Jellinek's perspective enables us to see society as a complex system of individuals with varying jural abilities/eligibilities. Throughout their lifetimes, the eligibilities of particular individuals will vary and will be enabled, disabled, or influenced by life events such as graduation, marriage, getting elected to a political position, conviction, and death. Certain life events will enable individuals to further progress on certain paths—to run for presidential elections, for example, will be possible only once a certain age has been reached; an insufficient educational level might prevent one from assuming a certain office; a conviction might prevent one from voting for a certain period of time; etc.

The levers of Jellinek's jural status are the titles, credits, certificates, and entitlements one receives throughout their lifetime, which enable individuals to wear different proverbial "hats." The academic pathway is one such paradigm of how one's shaping of their own jural status shapes the role they assume within the academic world. One collects certifications on passed exams as a prerequisite to obtain the desired academic degree; obtaining a higher-level academic degree requires one to have obtained a lower-level degree first; a teaching position enables one to influence others' progress on their own pathway by conducting and certifying various examinations, and so on.

6.2 HOHFELD'S ANALYSIS OF JURAL RELATIONS

Jellinek's theory of the system of subjective public rights argues for the existence of a system of subjects whose legally relevant interactions in their entirety constitute the political society. While Jellinek argues that the core expectation of the passive subject toward the state (i.e., the entirety of active subjects who constitute this state) is the claim-right for recognition and protection of *legally relevant allowed behavior*, Wesley N. Hohfeld set out to explore the nature of rights and the implications that their existence poses on society. Both base their work on the axiom that all jural relations are nothing but relations between jural subjects, though Hohfeld emphasizes that each jural relation is a relation between *exactly* two jural subjects.

Hohfeld is neither concerned by the legitimacy of jural relations, nor their moral justification, rather, his work merely aims to analyze their structure (Lazarev, 2005). This structure, according to Hohfeld, is built through four different jural relations defined by the correlatives *claim-right* ↔ *duty*, *liberty* ↔ *no-right, power* ↔ *liability,* and *immunity* ↔ *disability*. Fig. 6.1 visualizes the Hohfeldian relations, whereby the diagonally opposite concepts (i.e., claim-right vs. no-right, duty vs. liberty, power vs. disability, liability vs. immunity) are Hohfeldian jural opposites, which negate each other.

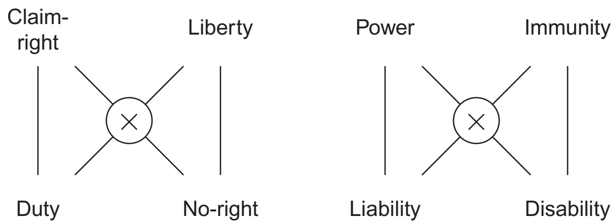

Fig. 6.1 ***Hohfeldian jural relations.*** The upper row contains the rights and the lower row their corresponding duties. The diagonal right/duty in each pair of jural correlatives are jural opposites, denoted here with the "x" in the relation.

This means, for example, that one's *liability* cannot coexist with one's *immunity* within the same bundle of relations. If Ann buys a house from Bob, then Bob's *liability* (to hand the house over to Ann) cancels out his *immunity* to continue to possess the house. Bob's *liability* to hand over the house to Ann is, at the same time, Ann's *power* to expect Bob's action of handing over the house. Should Bob not hand over the house, then Ann would have the *claim-right* toward Lea, the law enforcement agent, to assist in bringing the house to her possession. In the relation between Ann and Lea, Lea would have the *duty* to assist Ann.

Any entitlement to a specific person can thus be described through Hohfeldian jural relations, whereby the left-hand part of each correlative denotes the entitlement and the right-hand part the corresponding duty. A diagrammatic representation of this is given in Fig. 6.1. The flexibility of the application of these concepts allows us to model any complex real-world right through a multitude of jural relations, resulting in the so-called *bundle of sticks*.

A Hohfeldian *claim-right* is the entitlement to claim assistance or the withholding of action of another subject—the corresponding *duty* is the duty to assist or withhold from action, respectively. This right can be seen from two perspectives: on one side, it can be used directly on the private-law relation between two subjects, e.g., a subject has the right to claim withholding of action from a potential trespasser, or it can be seen as the entitlement to claim assistance from an authority to act, e.g., by punishing the said trespasser.

Hohfeldian *liberty* is nothing but the absence of a *duty* to withhold from action—what Jellinek calls *legally indifferent* behavior. Liberty, thus, is the liberty of unregulated actions such as singing songs in the shower, dreaming, or smoking in one's own home. The behavior exercised by an official within its Jellinekian active status, however, cannot be modeled as

Hohfeldian liberty, as that would fall under the category of a *duty*, which is the Jellinekian opposite of liberty.

Power is "one's ability to alter legal (or moral) relations" (Lazarev, 2005), such as the ability to acquire possession rights from another party (e.g., by purchasing them), whereby the latter becomes *liable* to act toward realizing the transfer. The jural opposite of liability is *immunity*, which means that the bearer of immunity is in a position which puts the correlate partner in a position of *disability*, and so cannot change the former's legal position. Such immunities are frequently expressed as constitutional elementary freedoms, which put the authorities in a position of *disability* when attempting to interfere with certain domains of their subject's behavior. For example, if Ann has *immunity* from surveillance by state authorities, then Lea, the law enforcement agent, would be in a position of *disability* to surveil Ann's telecommunications.

6.2.1 Applying Hohfeldian Jural Relations and Joining the Theories

Let us imagine *Ann* to be the owner of her house, and her neighbor *Tom* to be a trespasser who decides to walk over Ann's property out of sheer convenience. Let us further assume that law aims to protect Ann's *liberty* against Tom's *no-right* of trespassing by providing the law enforcement agent *Lea*. In this setting, Ann has the *claim-right* toward Lea to request protection, and Lea has the *duty* to provide it by, e.g., fining Tom if he continues to trespass on Ann's property against her will. (If Lea fails to carry out her *duty*, then Ann has the *claim-rights* toward state authorities superior to Lea, e.g., inspectorates, provided they exist.) Lea's behavior toward Tom is not her *liberty* toward Tom, but its jural opposite—*duty* toward Ann.

Tom, however, might wish to use his Hohfeldian *power* to alter his jural relations with Ann by making a deal with her in order to obtain the right to use her premises for transit. Ann, then (if they agreed on such transaction), would have the duty of *liability* to tolerate Tom's presence on her land. With this deal, Tom would get a *claim-right* toward Lea to recognize and protect his right if Ann suddenly decided to impede his agreed-upon transit.

Hohfeldian jural relations introduce details to Jellinek's model in the form of additional structure, but in general reconfirm the model. Both models emphasize a system of *fiat* eligibilities (Hohfeldian *claim-rights*, Jellinekian *positive status*), which subjects in their role of authority (Jellinekian *active status*) are to protect, generate, modify, etc., or, more specifically, to govern.

6.3 WHAT THEN IS "GOVERNANCE"?

The *Oxford English Dictionary* defines "governance," among others, as "the action or fact of governing a nation, a person, an activity, one's desires, etc.," whereby "governing" is defined as the action of directing and controlling the actions and affairs of a country/city/people/etc. More context-dependent definitions are provided by political science, where *governance* is a term with many heterogeneous meanings, as shall be outlined for the sake of completeness in Section 6.3.1.

The many different definitions from political science are, for the present treatise, of marginal value, and are mentioned merely for the sake of rigor. The reason for this is that political science (as a field of the social sciences) is about *observing* a (political/social) system's behavior, and hence, the terms and concepts used in political science are tools that serve that field's observational objectives. The role of technical sciences, however, is to *design* novel artifacts, and hence, when it comes to technicizing governance, the question to ask is not "what *is* governance," but rather "how can governance be *thought of* to be technicized."[6] This *technical perspective* shall be portrayed in Section 6.3.2.

6.3.1 A Myriad of Views

Governance is a highly vague, ambiguous term, the meaning of which depends on the context and the domain in which it is used. A comprehensive overview of different, highly heterogeneous notions as used in the domain of political and social sciences is provided in Mark Bevir's (2009) textbook *Key Concepts in Governance*, which identifies the meaning of *governance*, depending on the context. Below are a few notable context-dependent definitions (emphasis added):

- A "specific term to describe *changes in the nature and role of the state following the [neoliberal] public sector reforms* [, which] have led to a shift from a hierarchical bureaucracy towards a greater use of markets, quasimarkets, and networks [...] in the delivery of public services."
- "Some rational choice theorists [... have] adopted the concept of governance to refer to *norms and patterns of rule* that arise and persist even in the absence of an enforcing agent."
- "Social scientists have developed a concept of *governance as a complex and fragmented pattern of rule composed of multiplying networks.*"

[6] Jellinek (Section 6.1), being a jurist himself, likewise, did not ask himself the question "what *is* society," but rather "how can society *be thought of* so it can be handled by law."

- Radicals use the word governance "to describe *new systems of force and compulsion associated with neoliberalism*, and they use it to refer to *alternative conceptions of a nonstatist democratic order.*"
- "Joint-up *governance is as much about fostering networks as it is about managing them*."
- "All social and political regimes appear to depend on a pattern of rule, or form of governance, no matter how informal. Hence, the term *'governance' has come to refer to social and political orders other than the state.*"

These definitions do little to help one clearly understand the semantics of the word, but that again is not the point: Governance is no clear technical term, but rather a vague reference to an abstract concept, which only gains meaning once applied in a context.

Bevir further provides an overview of the main theories related to (societal/political) governance:

- The *rational choice theory* aims to explain public-domain action activities through the microlevel behavior of individuals who conduct the respective actions.
- The *new institutionalism* considers society to be a system of institutions, formal rules, procedures, organizations, norms, habits, and cultural customs, and studies the influences of these on public policy.
- The (sociological) *systems theory* studies governance as a self-organizing socio-cybernetic system composed of interdependent actors and institutions. In this context, *governing* refers to goal-oriented interventions, while *governance* refers to the total effect of governing interventions and interactions.

These theories help to model the (political/cultural) society for the discussions in political and social sciences. The *rational choice theory* is intertwined with the world view of Anthony Downs (Section 1.2.3) and aims to provide a model for understanding the behavior of individuals within the public apparatus, such as when one is in a position of power. *New institutionalism* focuses on concrete institutions and norms of the public apparatus, thus providing a framework that is able to take laws and policy documents into consideration.

Another theory explaining society is the *systems theory* (Ropohl, 2012). This theory is one that finds application in multiple domains of science, and is particularly noteworthy in the context of design science. Design science is the domain in which artifacts are designed and invented, and accordingly, it is also the domain in which *systems* are designed and invented. A *system*, in a nutshell, is something that consists of functionally connected, however, separable parts, each of which provides a function to the overall *system*. Characteristic to a system is that *a system is more than the sum of its parts*. A bicycle, for example, is a system: it consists of a frame, a saddle, a handlebar, two wheels, a drivetrain, etc. If assembled properly, the parts of the bicycle turn into a system which one can utilize as a means of transportation. This *systems thinking* is likewise a part of systems of law, systems of institutions, and other systems enabled by public policy.

A commonality of *governance* as shared through all these notions, definitions, and theories is the reference to an underlying system of principles, through which (social) functions of societies are orchestrated and steered.

6.3.2 A Technical View

The main objective of this treatise is to bring together knowledge to understand how public governance can be *informatized*. The result of informatization is a system which can be controlled from within cyberspace (Chapter 7 will elaborate on this). To this end, the question to ask at this point is how do these definitions from social science contribute to understanding governance in order for it to be informatized?

Scholars from political and social sciences may well be interested in understanding governance and governance systems in order to deduce knowledge about their implications on society or to understand the complex phenomena associated with their existence. However, their contributions to knowledge do not come as recipes or blueprints that give instructions on how to *informatize* governance, i.e., how to *control* it from within cyberspace.

The question that needs to be asked is *how can governance be thought of so that it can be informatized?* Unlike natural and behavioral sciences, which aim to understand and model natural or social systems, respectively, technical sciences aim to advance technical design by realizing new technical artifacts, or by improving them (Hevner et al., 2004; March and Smith, 1995; Wieringa, 2009). To *informatize* governance, therefore, conceptual levers must be identified, through which one can control governance by means of technical systems.

So, how can we *think of* governance to informatize it? The *river society* (Section 5.2) traversed a number of stages from *anarchy* (as in *no government*) at the beginning, to *absolute monarchy* with the rise of government at stage I, to *aristocratic oligarchy* in stage III with the inclusion of further stakeholders, to finally *representative democracy* in stage IV with the introduction of popular suffrage. These stages have little in common at first glance: the monarchic period required few rules, if any at all—the focus of the government was on levying taxes, for which no specific legal corpus was needed; by the period of representative democracy, however, the complexity of the society had risen to an extent where political processes, voting procedures, the rules of conduct in parliament, and the division of resources among the bureaus all required strict and formal governance in order to maintain stability. A closer look reveals that the underlying principles of operation remained consistent: the *system of tacit and explicit agreements and understandings* between the stakeholders governed the *subjective public rights* (cf. Jellinek—Section 6.1) within the society all the way from the birth of a public apparatus until its demise.

Tacit relations would be, for example, de facto power due to family ties and entanglement within networks of power. *Explicit* relations on the other hand are de jure contracts, symbols, or documents, which have relevance within a given societal (legal/political) system. While the nonexplicit nature of tacit relations between agents prevents them from being registered and structured, explicit relations can be structured and thus bear potential for becoming informatized.

By controlling formalized relations of governance systems, one ought to be able to influence the features and behavior of the system as such: if, for example, the possession of a symbolic item like a crown made its bearer the sovereign of the society, then a transfer of this symbolic item to another person would result in the transfer of sovereign authority. But rarely does one become king by simply coming into the physical possession of a crown, but, instead, the coronation would be the reflection of legitimacy.

The papal tiara, as the Shah's crown, is not more than a hyperexpensive piece of jewelry demonstrating one's access to the material riches of one's state. As the legitimacy of the Roman Catholic Church's *Pope* is given by the *College of Cardinals* and legitimacy of the Islamic Republic of Iran's *Supreme Leader* is given by the *Assembly of Experts*, so is the legitimacy of the US *President* given by the *Electoral College*, the legitimacy of the Chinese *General Secretary of the Communist Party* given by the *Central Committee*, and the Russian *President* given by popular vote.

Ultimately, the underlying *fiat* system is what defines how legitimacy is obtained and exercised, based on a system of formal positions and roles, which can be structured and informatized. Part III explores how these formalized relations in society can be *informatized*, i.e., controlled from within cyberspace.

REFERENCES

Bevir, M., 2009. Key Concepts in Governance. Sage.

Boyle, J., 1993. Legal realism and the social contract: Fuller's public jurisprudence of form private jurisprudence of substance. Cornell Law Rev. 78, 371.

Cerar, M., 1996. Večrazsežnost človekovih pravic in dolžnosti [Multidimensionality of Human Rights and Obligations]. Znanstveno in publicistično središče, Ljubljana.

Downs, A., 1967. Inside Bureaucracy. A Rand Corporation research study, Little, Brown, Boston, MA.

Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design science in information systems research. Manag. Inf. Syst. Q. 28, 6.

Hohfeld, W.N., 1920. Fundamental Legal Conceptions as Applied in Judicial Reasoning: And Other Legal Essays. Yale University Press, New Haven.

Jellinek, G., 1892. System der subjektiven öffentlichen Rechte, Elibron Classics Series 2006. Akademische Verlagsbuchhandlung von J.C.B. Mohr, Freiburg.

Jellinek, G., 1905. System der subjektiven öffentlichen Rechte [System of Subjective Public Rights]. JCB Mohr (P. Siebeck).

Johnson, D.R., 2007. Reflections on the bundle of rights. Vermont Law Rev. 32, 247.

Kersten, J., 2000. Georg Jellinek und die klassische Staatslehre [Georg Jellinek and the Classical Theory of the State]. Mohr Siebeck.

Kersten, J., 2011. Georg Jellinek's System—Eine Einleitung [Georg Jellinek's System—An Introduction]. In: System der subjektiven öffentlichen Rechte. Mohr Siebeck.

Lazarev, N., 2005. Hohfeld's analysis of rights: an essential approach to a conceptual and practical understanding of the nature of rights. Murdoch Univ. Electron. J. Law 12, 1–15.

March, S.T., Smith, G.F., 1995. Design and natural science research on information technology. Decis. Support. Syst. 15, 251–266. https://doi.org/10.1016/0167-9236(94)00041-2.

Ropohl, G., 2012. Allgemeine Systemtheorie: Einführung in transdisziplinäres Denken. Sigma, Berlin.

Smith, H.E., 2004. Exclusion and property rules in the law of nuisance. Virginia Law Rev. 90, 965–1049. https://doi.org/10.2307/3202415.

Smith, H.E., 2011. Property is not just a bundle of rights. Econ. J. Watch 8, 279–291.

Wieringa, R., 2009. Design science as nested problem solving. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, DESRIST'09. ACM, New York, NY, pp. 8:1–8:12. https://doi.org/10.1145/1555619.1555630.

PART III

Governing the Public Apparatus Through Technology

The objective of this part is to summarize the knowledge required on a conceptual level to understand how governance can be technicized in such way that it can be controlled from within cyberspace. The ability to control real-world structures from within cyberspace shall be called *informatization*—a term that is introduced in this treatise. This part is structured into five chapters, each of which covers important concepts and notions in the path to governance informatization.

Chapter 7 discusses how technology is deployed to control *structure*, as this is an integral part of systems such as physical systems (e.g., industrial machines), virtual systems (virtual worlds and other domains of the cyberspace), or *fiat* systems such as monetary systems and legal systems. It focuses on the four technological generations of controlling structure, which have led to technological and societal revolutions, such as the industrial revolution (caused by the introduction of automation of mechanized machines) or the revolution in society and business brought about by the emergence of the Web and caused by the introduction of informatization.

Chapter 8 addresses common pitfalls of the seemingly quick and easy introduction of technology into the context of governance, which fail to provide informatization in a timeless and sustainable manner; to this end, this chapter aims to debunk common myths of the abilities of trendy technologies bearing potential to cause more damage than good if applied to informatizing governance.

Chapter 9 analyzes the conceptual possibilities for informatizing governance that would adhere to the core principles of jural relations as discussed in Chapter 6. Following these findings, Chapter 10 elaborates on a conceptual multilayered architecture that would enable the informatization of governance. This conceptual architecture is an attempt to provide a center around which further research and design activities can evolve, to help bring new models of democracy to life.

Chapter 11, finally, aims to outline the enormous economic potentials of core technology, which, as is argued, is capable of providing a foundation for the emergence of grand-scale technological and societal ecosystems and economies, to nurture civilization for generations to come. It is this potential of core technology that provides justification for governance informatization to be considered an endeavor of ultimate sophistication and justifies further exploration and investment.

CHAPTER 7

Controlling Through Technology

Contents

Part II provided insights into the elemental structure of jural relations—that is, the rights and duties which legally bind individuals together. More specifically, theories of two legal scholars were introduced: Jellinek's *system of subjective private rights* and Hohfeld's *analysis of jural relations*. Jellinek explains the (legal) world we live in as a system, in which individuals interact with each other (in terms of law) based on their jural status, which in turn defines their role in society in relation to others. Accordingly, Jellinek's subjects assume positions depending on their situation, which put them in roles such as mayor, officer, professor, convict, and so on. What we learn from Hohfeld then is the atomic structure of legal relations, which reveals a discrete structure of eight possible entities that make up four types of binary legal relations, as described in Section 6.2.

The discrete structure of legal relations, which Jellinek and Hohfeld reveal, makes it possible to further consider how legal relations could be steered from within cyberspace—i.e., how they can be informatized. This chapter, then, aims to discuss on a conceptual level how this can be done.

The chapter is organized as follows: Section 7.1 outlines the four different generations of control by technology—mechanization, automation, computerization, and informatization. Section 7.2 explains how informatization differs from similar concepts such as computerization and

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00007-8

digitalization. Section 7.3 discusses the possibilities for controlling structure in the context of governance, based on the knowledge derived from the discussion in Part II.

7.1 THE FOUR GENERATIONS OF TECHNOLOGICAL CONTROL

From the second half of the 18th century to mid-20th century, humanity experienced radical transformations with respect to economic and societal prosperity, caused by an abundance of ground-breaking technological inventions. Economists and social scientists categorize and label these changes as three consequent industrial revolutions, with a fourth revolution conjured up by politics in the form of policy papers such as the German government's *Industrie 4.0* initiative, in which cyber-physical systems and the Internet of Things[1] are expected to transform industrial manufacturing (Bundesministerium für Bildung und Forschung, 2013).

The four industrial revolutions (the last yet to occur) serve as milestones in segmenting the evolution of society into distinct areas of time, in which various factors caused a chain reaction of memorable societal changes (defeudalization, urbanization, shuffles in economic and political power, changes in moral and societal values, etc.). However, they focus on fashions of production (e.g., conveyor belt and automation as facilitators of mass production), availability of new technical systems (e.g., cars, railroads, telecommunications, bicycles), or materials (iron, petroleum, paper), which are categories too broad to identify technologies that can trigger further transformations.

If we want to understand how technology can change industry, commerce, society, and societal governance, we must first understand which distinct features of technology can trigger change. An approach to identifying these triggers can be found in the *generations model*. In this model, the focus of observation is the manner in which structured processes are controlled. Four distinct generations are identified: mechanization, automation, computerization/digitalization, and informatization. Unlike the *revolutions model*, which deals with historic time spans, the *generations model* focuses on the maturation of a specific domain and its influence on fostering progress in others.

[1]The Internet of Things (IoT) is a term that refers to the practice of making small devices such as sensors, actuators, and machine-readable identifiers (barcodes or RFID tags) accessible through the Internet. IoT systems can then enable car sharing, advanced ticketing and tracking solutions, etc.

Mechanization and automation are not new constructs, but have been utilized since antiquity, as is known to us by the ninth century *Book of Ingenious Devices* by the Banū Mūsā.[2] Computerization, digitalization, and informatization on the other hand are only available for roughly two (or one) generations, being invented and realized during the prolific 20th century. This section aims to describe and demarcate these terms, to provide a normative understanding within the scope of this treatise.

7.1.1 First Generation: Mechanization

A basic approach to control structure is by means of *mechanization*. A mechanized system is a system whose functionality relies on interacting modules, whereby their interaction is enabled through human- or animal-based power. We can again use the example of the bicycle as a mechanical system—to operate it, one needs to physically push the pedals, pull the breaks, and steer using the handlebar. Another example is the pin-tumbler lock, where the manual insertion of the key aligns the pins in the right position so that the lock can be manually unlocked. Or the piano, where the manual pressing of keys sets a mechanism in motion, at the end of which there is a small padded hammer that strikes the corresponding string. Or the mechanical loom, a manually operated system for weaving, which introduced the concept of exchangeable punch cards to convey the weaving pattern.

The essential characteristic of these systems is that they involve multiple stages of operation, whereby the transition between the stages is conducted by physical labor. It is this very transition between stages that is of importance, as it is this characteristic which reflects *control*: the bicyclist can *control* the vehicle by increasing/decreasing speed, bringing it to a halt, etc.; the piano player *controls* the melody by pressing keys; the weaver *controls* the weaving output by changing patterns, controlling the dimensions of the woven textile, etc.

The transition between the stages, then, happens along determined, planned paths, which is one of the main properties of the mechanized system. Mechanized systems usually address existing functionality:

[2]The Banū Mūsā ("*Sons of Moses*") brothers are famous scholars from the Islamic Golden Age, who lived and worked in Baghdad, the capital of the Abbasid Caliphate. Besides their great contribution to astronomy and geometry, they contributed crucially to the preservation of Greek knowledge, which they translated and furthered, during the decline and fall of the Roman civilization. The *Book of Ingenious Devices* describes around a hundred different mechanical devices and automata, which encompass ancient Greek, Indian, Persian, and Chinese engineering.

The Persian santoor, like the piano, is operated by directly hitting strings with a hammer, though the piano features a complex multistage mechanism, which is triggered by pressing the key. The loom's functionality (weaving) had been addressed already by other nonmechanized looms for millennia, though the level of sophistication, the ability to increase precision and efficiency, and the ability to further advance the system in an unprecedented manner gave the mechanized loom its great added value.

The core principles of mechanization are the modularization of action, and the identification of mechanizable subprocesses. Modularization enables subtasks/subprocesses to be addressed and evolved separately from the entirety of the system. In case of the Jacquard loom, which today is regarded as a crucial step toward both industrialization and information technology (Keats, 2009), pattern design was not a *just-in-time* activity of the weaver, but has been outsourced to *programmed* subprocedures of a mechanical system. Likewise, the high specialization required to produce an accurate series of tones from the santoor has been leveraged to the array of strictly separated keys of the piano. The principle of splitting up activities and processes into subcomponents also plays a crucial role in the optimization of manufacturing and general work processes: division of labor into individually controllable subprocesses enabled the evolution of the assembly line, decentralized production, etc.

7.1.2 Second Generation: Automation (Power-Based Transitions)

Automation is the linked execution of processes, which as a whole comprise an automated system. While automation can be enabled, triggered, and controlled through many forms of forces ranging from manual labor to quantum-level processes, for the sake of the present treatise *automation* shall be distinguished from *mechanization* by the ability of a system to transition between states *without* requiring explicit manual or animal-based assistance during the transition. Thus, automation will typically involve the existence of a natural power source, such as wind, flowing water, temperature, pressure, steam, or a controlled power source like electricity. Accumulation of power, as in the electrical battery, the water tank, or the clock spring, can further serve as a power source to enable transition between states of a system.

Using automation to control a system enables modes of utilization beyond the abilities of mere mechanization. While the use of automation in production-oriented contexts boosts productivity, as in the case of the power loom or the automated assembly line, automation can be used to increase the power of devices such as the crane or lift, or the precision of a system as in the case of the clock or similar high-precision automata.

7.1.3 Third Generation: Computerization

The 20th century brought the digital computer (cf. the 1920s Lehmer sieve as an early nonelectronic digital computer) and electronics as a radical novelty to human knowledge. This new knowledge made it possible to invent and develop computerized systems for industrial production, which used digital computers and electronics for controlling manufacturing processes. The electronics which were used to control systems and processes could be steered by software, and in turn enabled a new quality of precision, as well as new possibilities for control of the technical systems involved.

Software enables a type of control that goes beyond mere automation. The 1980s book *In the Age of the Smart Machine* by Shoshanna Zuboff (1988) describes an inherent duality of software in steering complex industrial information systems. She describes how software is used to steer processes of computerized machines, keeping the state of the steered process in memory. As this software is aware of the state of the system, it can act accordingly. Zuboff calls this additional ability of software *informating*. Her use of *informating* thus refers to the inherent context awareness of systems, which have been designed in such a way that the software not only steers their performance, but also generates, stores, and uses information about the context: "The programmable controller not only tells the machine what to do—imposing information that guides operation equipment—but also tells what the machine has done—translating the production process and making it visible" (Zuboff, 1988, p. 10).

Zuboff's fascination for the duality of information technology is comprehensible if one takes into account her era, in which a radically novel generation for controlling structured processes emerged. However, from a 21st century perspective, this fascination has faded out, as software controllers (and their inherent state awareness) have become normal in engineering and management in the digital age. Zuboff's informated *Smart Machine* not only automates processes of production, as *second generation* machines were capable of, but is also aware of its own current state within the context. It is therefore a machine managed by *third generation* controllers whose primary objective is to *automate* specific processes (such as soldering car parts, harvesting crops, calculating salaries, or counting votes), while the machine's state awareness enables an unprecedented level of precision and complexity.

The defining characteristic of the *third generation* of control is thus the use of the *computer* as a device which processes data, acts upon information, and composes instructions to context-consciously govern the process(es) of the system it controls. This level of control is best called *computerization*—such a system is then *computerized*. Typical examples of computerized systems are industrial robots, automotive electronics, computer-steered domestic appliances (fridge, dishwasher, electric stove, air conditioning), etc.

7.1.4 Fourth Generation: Informatization

Both *computerized*, as well as *informatized* systems, are based on software. However, the use and purpose of the software differ significantly. In computerized systems, software is used with a focus on efficiency and utility of the systems' functionality. Informatized systems on the other hand use software to enrich the functionality of the system at runtime and allow room for enhancement beyond the limits of the systems' original design. With informatization comes the leap into cyberspace and the creation of new forms of interaction, production, and perception.

The *computerization* of the piano yielded the electronic keyboard—not only is it significantly cheaper to produce, but it can also provide advanced functionality such as different categories of tones, direct coupling to sound processing devices, etc. However, the *informatization* of the piano's functionality goes beyond the provision of electronic tones. Standards such as the *music instrument digital interface* (MIDI) are about composing tones and tunes purely in cyberspace, where they can be controlled and transformed through a myriad of tools and communicated through various systems while remaining as an informatized melody that can be heard in the real world. The result of a system's informatization is thus informatized entities, which can be created, controlled, and transformed within cyberspace. The informatized entity can then be rendered into the real world from cyberspace and generates a real-world effect—the informatized melody would be the basis for a real-world melody to come to life.

Another example is the *portable document format* (PDF), which plays a significant role in informatized production in the scope of desktop publishing. The PDF file contains all of the data required to ensure an accurate rendering of a document onto a two-dimensional (2D) surface; to this extent, it contains the fonts, the text, the vector graphics, the arrangement of the elements on the 2D canvas, the color spectrum definition, and so on. The free availability of the specifications[3] allows PDF files to be viewed on almost every computer platform and used in the workflows of desktop publishing from the stage of design to print.

7.2 HOW INFORMATIZATION DIFFERS FROM DIGITALIZATION, VIRTUALIZATION, ETC.

Informatization must not be confused with similar terms like *virtualization*, *digitization, digitalization*, or *computerization* (Fig. 7.1). *Informatization* is a term which we use deliberately to denote the quality and characteristics of technical control of a certain thing by means of information technology from *within* cyberspace. Let us first take a look at these terms to clarify the semantics.

According to the *Oxford English Dictionary* (OED), *to virtualize* means to make a "virtual version of (a computing resource or facility)," or "to convert to a computerized or digitized form; to make a computer-generated simulation of; to conduct using computer technology rather than more traditional means." A *virtualized* thing is thus a simulation/imitation of something as represented in a computer system, for example, a virtualized airplane in an airplane simulator. This entity then lives entirely in the virtual dimension of its hosting environment (e.g., the computer game as such), without any real-world effect (a virtual plane crash will not hurt its

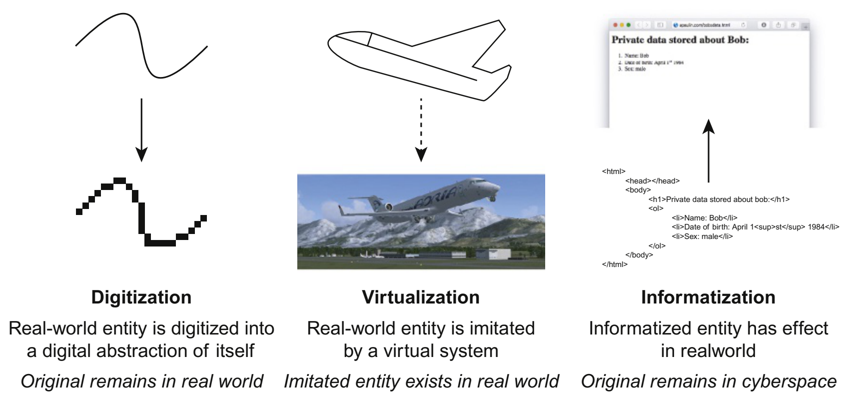

Fig. 7.1 Digitized and virtualized entities/concepts originate from the real world and reflect in cyberspace. Informatized entities reverse this relation: they originate in cyberspace, causing effect in the real world.

[3]The PDF format has been developed as a proprietary specification by Adobe in the 1990s, which made the specification available free of charge in 1993. In 2008, the specification was released as an open standard, published as ISO 32000-1.

real-world pilot). Other examples are virtualized system components, such as virtualized hardware resources used in cloud computing, or virtualized software platforms, such as virtual PCs. To this end, hardware resources are imitated using software and are virtual—i.e., *unreal*. Nevertheless, the systems that run inside such virtualized environments act and perform as if the virtualized components physically exist. Likewise, when engaging with computer games, the players act as if they would be interacting with real environments, though everything they do exists solely in cyberspace.

To *digitize*, the OED explains, means to "convert (analogue data, esp. in later use images, video, or text) to digital form, typically for storage or processing by a computer; to represent in digital form." A singer's song, for example, will be digitized so that it can be processed by digital systems. In nature, a song is an *analogue* acoustic phenomenon—this means that the sound waves that make up the sound are continuous, i.e., they are true waves. But when the sound wave is *digitized*, it is converted into a digital representation of discrete values, i.e., there is no longer a wave, but a series of "steps," which follow one after the other. The *digitized* sound is thus a *virtualized* entity of its former self and therefore any alteration of the digitized sound has no effect on the real-world original.

To *computerize*, according to the OED, means to "prepare or adapt (a system, activity, function, etc.) to operate or be operated by computer; to equip with a computer or computers." A computerized land registry is thus a land registry which was formerly paper based, but has been rebuilt as a computerized (more correctly, digitalized) system. Again here, this concept emphasizes the disconnection between the original and its *computerized* version.

Many scholars instead of *digitalization* use the semantically largely overlapping, if not fully synonymous, term *computerization*. The problem with these terms is that they lack precision. *Digitalization* is frequently used to refer to the use of information and communication technologies for business/administration (Katsikas and Gritzalis, 2017), and is defined as such by the OED: "The adoption or increase in use of digital or computer technology by an organization, industry, country, etc." Other sources use it as a synonym for *digitization*, an established technical term to refer to the transformation of analogue signals (or real-world items) into a digital representation. On the other hand, *computerization*[4] implies a closer proximity to software for directly controlling hardware. Accordingly, we suggest the following use:

[4]OED: "*The action or process of computerizing an organization, activity, etc.; the conversion of information, text, etc., into a form which can be stored or processed by computer*" (Oxford English Dictionary, 2010)—note the proximity to *digitization*! Oxford Dictionary of English (ODE): "*convert (a system, device, etc.) to be operated by computer: the advantages of computerized accounting.*"

electronics in the car and dishwasher make them *computerized* systems, while the use of accounting software makes a business *digitalized*.

The word *informatization* is defined by OED as "the adoption of information technology; computerization." The problem with these existing semantics is that three different words (*informatization, digitalization, computerization*) all vaguely stand for the same thing—namely the use of an ambiguous mixture of information technology (software), digital computers (software + hardware), and electronics (hardware) in a given context (or the introduction of such). For the sake of professional clarity in the use of these words, the terms *informatizing/informatization/informatized* should be used solely in the context of *fourth generation* systems as described herein.

7.2.1 The Role of the Computer File

The defining novelty of the *fourth generation* lies in the reliance on the *digital (computer) file* as the descriptor of a system's (or digital object's) characteristics and state. More specifically, the type of *file* at stake is the type which can be exchanged, shared, edited. While the computer file as a concept to store a system's state has been known since the 1950s, it is only the later evolution of file systems as a part of widespread computer operating systems and files in the form of standardized, open file types which enabled the *fourth generation*.

The modern computer file constitutes digital objects in their *serialized* (i.e., written down in digitally readable structure) form. Computer programs *deserialize* the information contained within the file and make use of the data/information/instructions. The way in which a given file is used depends entirely on the system it is used by. A *file* can be a composition of graphic elements, a plug-in for a computer program, or a software library that extends the functionality of a computer program. A PDF file, for example, can be composed by a digital artist (and edited by their peers) using desktop publishing software such as Adobe Illustrator—this file will then contain a logical composition of graphics and text, which can be interpreted by other software to instruct display hardware to render the graphical composition on the computer screen. The very same file can then be transferred to a printing software, which will instruct printing hardware to create a tangible instance of the digital graphic. During all stages, the file from this example remains the *original* digital object, which can be created, edited, deserialized, shared, copied, transformed, rendered to a human-perceptible representation, etc., in a potentially indefinite number of ways.

The PDF file is an excellent example of an informatized entity. The file is created using software right on the desktop, which makes it a native entity of cyberspace. For example, graphic designers can use the Adobe Illustrator software to create vector drawings or graphical layouts, and can store these as PDFs without losing the capacity to manipulate the files later on, using either the very same software or a similar one. Alternately, content can be created using a word processing software such as Microsoft Word or Open Office, professional print layout tools like Adobe InDesign or QuarkXPress, or in LaTeX[5] and distilled into a PDF file. The PDF file which has been forged will then provide screen-rendering software instructions on how to visualize it to be viewed on screen; it can be shared over the Internet, put online, or, if printed, will provide instructions to the printing system on where to draw lines, or cut the paper, to yield flawless prints of any technically doable size.

The *original* file will be the PDF, a native of cyberspace that exists as a perfect *informatized* description of itself, which then can be brought into the *real world* as an instantiation. Unlike *virtualization*, which imitates a *real-world* entity within cyberspace, and unlike *digitization*, which translates an analogue entity from the real world into a digitized entity in cyberspace, *informatization* originates (!) from within cyberspace and can be *rendered* into the *real world*.

Other examples of thoroughly informatized systems are the Web's technology stack (HTTP, HTML, CSS) or the *open document format* (ODF), which provides a common format framework for word processing software to store their files in. Developer frameworks like .NET and Java, or platforms such as the Java-based Android, are examples of different types of informatized systems on top of which software engineers craft further computerized, digitalized, and informatized systems. Platforms like Facebook, Wolfram Alpha, or Google are other examples of systems which provide Web-based access to their functionality for the peer production of additional computerized/digitalized or informatized systems on top of them.

The common component of informatized systems is that they have a multilevel access to the system as a feature of their design. An informatized letter, for example, would be composed using word processing software and stored as an ODF. In the word processing software, it would be displayed as a neatly typeset document. Under the hood, however, lies a zipped structure of folders and files, which describe how the document *can* (or rather *should*) be visualized. Likewise, while most users might interact with a Web page

[5]A typesetting system popular in hard sciences due to its strong capabilities in dealing with mathematical equations.

using a Web browser of their choice, the browser is only one option to interact with the system. In the case of developer frameworks, the multilevel access is assured through the shareability of programming libraries, while Web-based platforms offer dedicated APIs for developers to access the functionality provided by these platforms.

In order to be able to instantly cowork on a file, networked work spaces (computers with the required software) among which the file can be shared are of advantage. The sharing of files that contain virtual compositions (graphics, multimedia), software systems/components (executable code), or other types of digital objects enables the emergence of virtual coproductive communities, which rely on cyberspace as a gathering environment (cf. Raymond, 1999). This emergence of cyberspace in terms of a dimension for interaction, production, and creation of value (online services, etc.) is in itself another enabler of the *fourth generation* for controlling structure. Although, at the end of the day, all interaction in cyberspace is nothing but an exchange of data between terminal equipment, this interaction is so different in quality and complexity that it must be distinguished from plain exchange of signals/data as it occurs in telephone calls or telemetric readings. Nora and Minc, forecasting the upcoming change of quality of information and communication technologies in the years of the emerging Internet, coined the word *telematics* in their report *The Computerization of Society* (Nora and Minc, 1980; Shanken, 2000). Although the word *telematics* (as well as the prefix *tele-*) has gone out of fashion, the justification for the then-new word *telematics* is a relevant indicator of substantial change in the generation of technology.

The modern file is thus more than a mere representation of a system's state (as the early computer file was) and more than a set of processing instructions (as would be sufficient for purposes of automating and informating a system)—it is a genuine object, which exists natively in its digital form, and only when interpreted by software descends from cyberspace to the physical world (in perceptible form as printouts/products/visualizations/music/movies or actions such as granted access to resources, movements of robot arms).

7.3 INFORMATIZING GOVERNANCE—TECHNOLOGICAL LEVERS

In order to be able to control and steer the provision of a certain function, levers must be identified and accessible. The evolution of a controllable structure was illustrated in Section 7.1 using the evolution of music: the *nonmechanized* santoor, the *mechanized* piano, the *computerized* keyboard, and finally the *informatized* MIDI tune. In all these cases, the tune was the outcome of the system's operation and the system's structure was designed in order serve that outcome.

The santoor defined a core structure: string and hammer to produce the sound, know-how of its operation, and the melody as a result. The piano mechanized and extended the hammer and string structure, changed the required skillset, but keeps the melody as a result. The resulting system was a highly sophisticated, though bulky and superexpensive device, which is costly to manufacture and maintain. The keyboard replaced the string and hammer for electric signals, while keeping everything else as it was, thus making the piano accessible to the masses and making it cheap, portable, and zero-maintenance. Lastly, the MIDI format moved the tune to cyberspace, replacing hardware for software to provide the core functionality of a music device. While previous generations focused on replacing tangible components of the music device to make changes happen, informatized music brought about a new system and new structure to write down the tune itself.

If we are to informatize governance, then the question to ask is: What are *governance*'s hammers and strings, or musical notes, that can be transformed to transfer governance into cyberspace?

7.3.1 Summary of the Theoretical Framework

Part II aimed to explore the conceptual possibilities for informatizing governance, i.e., to provide a core understanding about constraints and implications of governance systems for their ability to be informatized. It addressed questions of how systems of power arise and evolve, how governance comes to be, and how formal systems of law govern legal relations within a society.

To illustrate the emergence of government, its transition into a public apparatus, and the role of individual actors in the growth and perpetuation of governance, we presented in Section 5.2 a thought experiment in which a society grows from the need to cross a river. In that thought experiment, a private entrepreneur provided a raft-based service for crossing the river, which later was put out of business due the construction of a bridge. The bridge was nationalized and taxation was introduced to provide for renovation and maintenance of the bridge, as well as for the existence of a government. With the introduction of taxation, many different appetites emerged, forcing the government to transform and open up, giving rise to institutions such as a parliament and suffrage. Soon ministries and other bureaus emerged that provided new social functions from domains such as security, education, and health care, and lastly, a civil society made the transition to a public apparatus complete.

Governance, as revealed through that experiment, could best be defined as a *system of tacit and explicit agreements and understandings between agents*, hence, a *fiat* system, which existed so long as the involved agents continued to support it. This definition was compared to disciplinary definitions from social sciences and found compatible. While tacit agreements are without formal structure (e.g., terms of a friendship cannot be structured and enforced), explicit agreements can be recorded and can serve as a base to enforce entitlements that would stem from them (borders of a land parcel, for example, can be recorded, to enable sanctioning of trespassing).

Those agreements and relations which can be structured can then be controlled in some way. The structure of such explicit relations has been revealed by the theories of Jellinek and Hohfeld, who teach us that one's role in society is defined by its jural status (according to Jellinek), while concrete situations of interaction of two "people" are defined by the bundle of rights.

The "hammers and strings" of governance are thus the explicit and recordable jural relations between individuals, as well as the proverbial "hats" which individuals hold in order to be able to exercise their respective power. In order to reach the objective of informatizing governance—i.e., to transfer the control and steering of governance into cyberspace, our task boils down to the question: How can those proverbial "hats," and the other information that make up jural relations, be informatized?

7.3.2 Informatizing Jural Relations and Jural Statuses

The good thing about explicit relations among people is that they can be recorded in one way or the other. This means that all jural relations bound to the jural status of a subject can be reduced down to plain *data*, which can easily be stored in a digital form and represented within a software system. Let's take a look at the following example.

The mayor of a town has undergone an arduous journey to reach this position. The aspirant had to make a myriad of deals with stakeholders who influence the voters, had to register as a candidate, had to endure public attention, had to get elected, and had to be confirmed in a ceremonial procedure following victory at the elections. Throughout this journey, various committees made assertions as part of their governance of the election process. In order to run for office, the mayor candidate first had to register with the election commission, which had to confirm the candidate's fulfillment of the requirements. This commission registered the cast votes, counted the votes, and asserted the validity of the elections. Finally, the new mayor was inaugurated by the town council. This last act gave the new mayor the proverbial "hat," by which the mayor gained access to the new privileges—the new *rights*.

Accordingly, the origin of the mayor's new set of *legally relevant allowed behaviors* is not found in the voting (that would be the ideological origins of the mayor's legitimacy), but rather in the town council's inaugural decision, recorded in the form of a formal decree issued by the election commission declaring the candidate as the winner. If the commission was to revoke its former decision—say, if they were to find that the elections were rigged—then the mayor's set of *legally relevant allowed behaviors* would instantly return to its previous circumstance, i.e., the mayor would instantly cease to be mayor.

And this is where the technical lever to control governance by means of technology can be found. Fig. 7.2 aims to illustrate this: it is the organization with power (the hegemony—the government agency, the judge, and so on) which creates a *right* out of free will, i.e., out of its Hohfeldian *power*. This right then is materialized in one way or another—i.e., put in the form of a formal notice, a decree, or a certificate, which reflects its existence.

A token asserting the existence of a right can then either be digitized (e.g., scanned) or be virtualized (i.e., recorded in a database), or it can exist

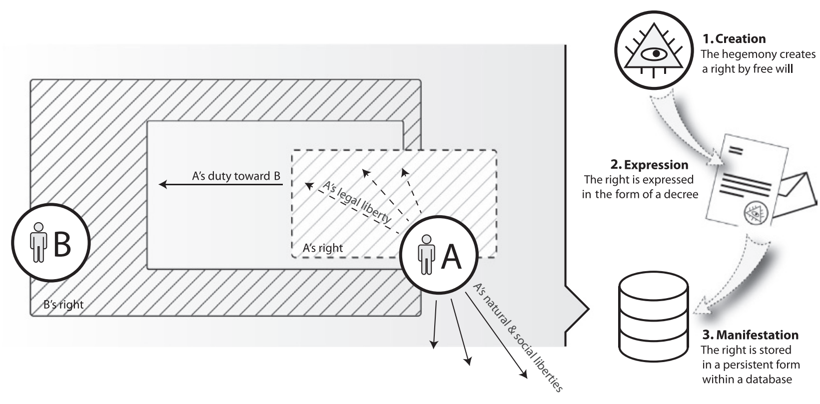

Fig. 7.2 ***The anatomy of jural relations.*** Informatized or virtualized assertions can serve as a source of legal relations.

as an informatized entity—i.e., the information would originate from cyberspace. Whereas a digitized or virtualized token would be only a copy of the original, an informatized token would be *the* original from which one's set of legally relevant allowed behaviors would be derived.

Creating informatized tokens, revoking them, or modifying them would then enable the exercising of control over the *subjective public rights* that stem from these informatized tokens. This way, governance can be informatized, i.e., the explicit and formalized relations on which de jure power are based could be steered and controlled from within cyberspace.

Taking this lever into consideration, we can further explore the construction of an IT system that would take into consideration the following guidelines: First, it would have to *virtualize* subjects (individual people, as well as legal persons, such as organizations) and thus abstractly represent their existence in the IT system. Next, it would need to store the legal statuses of these subjects as assertions (e.g., certificates, decrees) in their *informatized* form in the IT system, to govern them from within cyberspace. Finally, all other public resources, which can be recorded in an *informatized* form, such as public funds or concessions, should be stored in the system.

Today, information such as decrees and rights are stored in digital form in the form of scans or database entries. However, this fundamentally differs from storing them in an informatized form. While a scan (a digitized version) or a database entry (a virtualized version) of such tokens serves well in digitalized processes, they remain virtual representations in cyberspace of their real-world originals. A change or destruction of such virtual representations might lead to confusion (e.g., in reporting), but would have as much of an effect on the original as a virtual plane crash in an airplane simulator game—that is to say, none. The virtualized token is enough to enable screen- and system-level bureaucracies, where administrative decisions are made remotely, or even automatically, but is of no use in enabling the next generation of governance.

Informatized systems of handling legal relations and legal statuses would enable informatized governance—i.e., the controlling and steering of systems of governance through cyberspace. This would mean a leap into the *fourth generation* of controlling governance and would open new opportunities for the development of dedicated technology and its standardization, as well as new forms of stakeholder interaction, etc. The opportunities afforded by informatized governance, and the technological implications, shall be explored in following chapters.

REFERENCES

Bundesministerium für Bildung und Forschung, 2013. Zukunftsbild "Industrie 4.0."

Katsikas, S.K., Gritzalis, S., 2017. Digitalization in Greece: state of play, barriers, challenges, solutions. In: Paulin, A.A., Anthopoulos, L.G., Reddick, C.G. (Eds.), Beyond Bureaucracy. Springer International Publishing, Cham, pp. 355–375. https://doi.org/10.1007/978-3-319-54142-6_19.

Keats, J., 2009. The mechanical loom. Sci. Am. 301, 88.

Nora, S., Minc, A., 1980. The Computerization of Society: A Report to the President of France, pr. ed. vol. 2. MIT Press, Cambridge, MA.

Oxford English Dictionary, 2010. Computerization, n. Oxford English Dictionary.

Raymond, E.S., 1999. The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary. O'Reilly Media.

Shanken, E.A., 2000. Tele-agency: telematics, telerobotics, and the art of meaning. Art J. 59, 64. https://doi.org/10.2307/778102.

Zuboff, S., 1988. In the Age of the Smart Machine: The Future of Work and Power. Basic Books, New York.

CHAPTER 8

Semantic Technologies, Algorithmic Governance, and Platforms

Contents

Informatizing governance is a grand vision for a future in which a community can steer and control their governance through cyberspace. By this means, they could control their providers of social services, their authorities, their public policies, their laws and judiciary, among other things that fall in the scope of public governance. While informatizing governance is not meant to be limited to steering and controlling concrete functions and services, it is necessary to test and discuss its value against features, functions, and outputs of existing agents that make up (public) governance as we know it today.

When discussing governance informatization with fellow researchers from computer science and informatics, the discussion inevitably turns to clumsy interpretation of real-world examples taken for illustration, and simply reduces the complexity of the challenge to the level of concrete contemporary problems or scenarios. As soon as this level is reached, premature solutions that follow well-known patterns of problem-solving are quickly offered; however, on further inspection, they fail to solve the challenges satisfactorily. One reason for this is easily explained: The IT community is a community of engineers who often share an intrinsic handicap, namely, the urge to get things done. There is no doubt that it is valuable if an engineer is able to solve a problem quickly and efficiently. However, this very natural urge is a significant stumbling block when designing and

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00008-X

developing for broader visions, or when it comes to producing systems of higher virtue that would require input from several generations. The result is narrow-minded action, marketing-level buzzwords, and a vivid dynamic of professional terminology, which contributes more to confusion than to progress (cf. Chapter 2).

This is not to say that this urge to *get things done* does not yield innovation. To the contrary, the very same urge paired with the ambition of individuals has resulted in the paradigm of peer production[1] that gave birth to the Internet, the Web, and the technologies and products that brought cyberspace to life. This is also not to say that there are no grand visions in the domain of IT. Tim Berners-Lee's *Web/Semantic Web/Linked Data on the Web* complex of interlinked data and "smart" relations is a good example of a grand vision set in cyberspace. Another is Tim O'Reilly's *Government as a Platform/Open Data* school of thought that follows similar ambitions. The *Internet of Things* (IoT) is another example. IoT is used, for example, in smart home systems that enable remote control of heating or smart cars used by car sharing companies to control locks, authenticate drivers, read gas levels, or personalize navigation destination. However, the IoT is less of a vision (it lacks a grand objective), but more of a general idea—*telemetrics*, *cybernetics*, and *ubiquitous computing* essentially followed the same idea of remote controlling physical things/systems, and have been discussed since 1960 (Nora and Minc, 1980; Peters, 2016).

These ideas for the engineering of gigantic networks of semantically annotated and linked information, the engineering of a platform for accessing services of government, and the associated idea to make governance happen by means of algorithms and/or artificial intelligence are suggestions that come naturally as approaches to technicize governance. However, these ideas are of marginal significance to the objectives of governance informatization, as shall be discussed in this chapter.

Section 8.1 provides a discussion on the use of semantic technologies as suggested by Berners-Lee's grand vision of the evolution of the Web. Section 8.2 discusses the concept of the government platform as suggested by O'Reilly (among others), as well as the concept of algorithmic governance, which such a platform would imply. These discussions aim to contribute to identifying the capabilities and limitations of a grand vision of governance informatization, as shall be concluded in Section 8.3.

[1]Peer production is a way of producing goods and services that relies on self-organizing communities of individuals.

8.1 SEMANTIC TECHNOLOGIES

Hohfeld's (1920) jural relations (Section 6.2) are a relevant conceptual tool in distinguishing various types of rights and duties that in their entirety constitute legal relations between subjects within the domain of, e.g., a state. Jellinek's (1905) concept of subjectivity and jural statuses (Section 6.1) is not a conflicting theory, but rather both theories complement each other and share the goal of structuring jural relations between subjects in a shared political/legal space. The world which Jellinek and Hohfeld describe is a network in which subjects are the nodes and jural relations are the links between those nodes (whereby links depend on the jural status of the participating subject nodes).

If jural relations (hence, also those which constitute governance) are a network, then it should be easy to informatize it, right? On first glance, it seems both intuitive and feasible to use the tools and know-how from informatics to transfer these relations into cyberspace, where they would then reside as informatized entities, and thus could be steered and controlled. Let us take a look at what this would mean: In Section 6.2.1 we outlined a conflict between land owner Ann and trespasser Tom, where Ann requested help from law enforcement agent Lea. The relation between Ann and Tom was the Hohfeldian correlate *A:liberty* ↔ *T:no-right*; the relation between Ann and Lea was *A:claim-right* ↔ *L:duty*. Other than that, there are several semantically describable concepts present in this dispute, such as *ownership*, *land parcel, officer, and trespasser*. Accordingly, we could model these relations in cyberspace by virtualizing Ann, Tom, and Lea, as well as Ann's land parcel. A link between Ann and her land parcel would express ownership. Links between Ann, her land parcel, and any other person *P* would denote a relation of type *A:liberty* ↔ *P:no-right*. If Tom trespassed on Ann's property, Ann would establish a relation between her and Lea of type *A:claim-right* ↔ *L:duty*, calling for protection, etc.

Modern informatics offers a plethora of research under the term *Semantic Web*, if one wishes to go for the low-hanging fruit in this context. The idea of the Semantic Web is that data and services (together: resources) are available on the Web and interlinked through a system of metadata, which *semantically* describes each resource by means of vocabularies (which are called *ontologies*). These vocabularies contain terms used to categorize (hence, understand) the resources and the relations between them, which is useful for applications of artificial intelligence, for automated discovery and analysis of contents, and the kind.

Semantic technology could thus be used to erect a network of virtualized subjects in cyberspace, whereby the relations between the subjects would be described semantically in the form of Hohfeldian jural relations. At first glance, such an endeavor would be highly complex, but not necessarily undoable. Let us consider the relation between the state and its taxpayers (subjects of type "natural person" or of type "legal person"): each taxpayer has the Hohfeldian *duty* to pay, e.g., 50% tax from their annual net taxable income, which corresponds to the *claim-right* of the state to demand payment of taxes. In this fashion, a really complex and gigantic network of relations could be established, which would contain the information of how much each subject owes the state.

Semantic technologies are incredibly proficient in producing statements such as "Ann must pay her government €20,000 tax, because her income was €40,000 and the tax rate is 50%." Statements like these are the cornerstone of logical reasoning in artificial intelligence, and find great application in the understanding of free-text queries by Web search engines, knowledge engines such as Wolfram Alpha, or *knowledge navigators* like Apple's Siri. But that then is pretty much it. Describing each and every jural relation between subjects in a network of jural relations through semantic technologies would be a very naive approach, as only a coarse set of ambiguous meanings can be conveyed in this way. It is logically impossible to perfectly describe a relation between resources from the digital realm using terms borrowed from a natural language—it is, after all, impossible to even accurately translate the complexity of context-dependent meaning between two natural languages (cf. Sharifian, 2007).

Semantically enabled artifacts such as those experimented with in e-Gov (Vitvar et al., 2010) use resource-describing semantics, which aim to truly semantically *describe* the resource and its relations. This means, for example, that a catalogue of information will provide a description about the data it offers in a machine-readable way. We can call this approach *deep semantics*.

However, deep semantics are strongly dependent on the context. In this book, so far, we discussed two words whose meanings are very different depending on who one might ask: Section 1.1.1 asked the question "what is the bureaucracy?" and Section 6.3 aimed to unravel the meaning of "governance." So, if we were to semantically label a person as a "bureaucrat," what would that mean? Is such person a member of an emerging 17th century *bureaucratic class* striving for power and privilege, or poorly paid 21st century *public official*? Then, there are words whose semantics are closely overlapping, if not fully synonymous, such as *computerization* and *digitalization*, which were discussed in Section 7.2. Further issues with deep semantics are revealed when attempting to translate semantic concepts into different languages, or from one cultural space into another—e.g., from British English (BE) to American English (AE). The word "smart" in BE for example is used predominantly to describe appearance, meaning elegant/neat/stylish, while in AE "smart" describes mental abilities such as clever/showing intelligence/quick at learning (Khazan, 2016).

On the other hand, the use of deep semantics can make sense within closed application domains, such as within the scope of national states and use of the official language. Kowalski's (1992) experiment to model British immigration law as a computer program, for example, used deep semantics for the automated reasoning logic. This was feasible as the experiments were clearly confined to official English, and modeled a clear use case in a laboratory environment.

The theories of Jellinek and Hohfeld suggest to perceive the relations between jural subjects in the form of bundles of different relations among two or more people. The content of each of these relations are jural entities, which can be things, other subjects, other rights, etc. In the example from Section 6.2.1, the protection requested from Lea against Tom's trespassing on Ann's premises is the content of Ann's Hohfeldian claim-right toward Lea. These bundles of rights could hypothetically be described using a finite set of discrete types of links between jural subjects and jural entities.

To describe the links, Hohfeldian legal relations (correlates, opposites) could be used, whereby the features of each subject's Jellinekian status would determine which Hohfeldian legal relations a person could establish with another. This would result in a vast network in cyberspace, whose nodes would be the virtualized subjects and virtualized legal entities (both represented through unique identifiers), and the links would be Hohfeldian legal relations. This network would be composed of only these discrete links, while their real-world meaning would be dependent on the context of a given situation. Thus, instead of describing the real-world action stemming from a certain relation (e.g., Lea's duty toward Ann to protect her interest against Tom's trespassing) by means of deep semantics, it would be up to the context-aware agent to understand how to act. In the case of Ann's claim-right toward Lea for protection of her liberty against Tom's trespassing of her property, it would be up to Lea to act according to her duty as imposed by the context of the law. While in this case the relations are still described by means of semantics, these semantics are limited to a fixed set of elemental constants, whose meaning can be defined on a technical level. This type of semantics shall be called *shallow semantics.*

While it appears to be straightforward to create such a network of semantic links between subjects, this could only really work on the level of laboratory experiments. The sheer complexity of such a network would make it technically unmaintainable. It would take a myriad of links between all subjects and entities in the network to accurately represent every relation, and each addition of a new subject or entity to the network, or the change of a subject's jural status, would require the entire network to be updated.

Both deep and shallow semantics fail to provide a feasible mechanism to represent jural relations as what they are—a complex fabric of perpetually changing relations between jural subjects. If we were to use semantics to denote rights or types of rights, we'd unavoidably be chasing the white rabbit into its borrow. There are two main issues: one is the evolution of one's legal position in the fabric of legal relations and the other is that semantics remain dependent on context and culture. For example, the concept of the *claim-right*, as is used in Western thought is a rather modern concept. The Western concept of rights was introduced to cultures within the Middle and Far East only when modern Western civilization spread globally. Hinduism, Confucianism, Judaism, or Islam knew *rights* only in the form of *duties* and faced the Western concept of *rights* only when dealing with it in scholarly debates. When the Japanese and the Chinese modernized their legal systems in the second half of 19th century based on the French Civil Code, they had to invent new words in order to adequately introduce the Western concept of *rights* into their legal culture (Cerar, 1996, p. 72). Some indigenous African tribes still have no concept of land property (Cerar, 1996, p. 97; Wähler in: Cerar, 1996, n. 49), but think instead in terms of tribal territories.

Though cultures spanning from primitive tribes to advanced civilizations had not used explicit terminology to express *claim-rights*, it does not mean that they did not know of the concept which we associate with this term (Cerar, 1996). If they used different semantics to describe these concepts than we do, then we can assume that our successors might again use different words for the same thing. Accordingly, if each culture can be expected to use different semantics for the same concepts, then semantic labels cannot be used sustainably to describe the concrete relations of a global network of jural rights.

Virtualizing jural relations and expressing them through a network of semantic relations can be used to model a snapshot of a society at a given point in time. Such models then can be used to conduct simulations of the behavior of a society. However, to model a continuously evolving society becomes unfeasible. Such virtualization of jural relations does not contribute to informatizing governance—i.e., making the jural relations controllable from cyberspace. A system that would enable informatization of governance must therefore not rely on predefined semantics, but rather must be designed in such way that the stored information and relations are interpreted by the users of such a system.

Accordingly, the system sought for governance informatization must be *generic* and *modular*, in order to be able to absorb the changes of the context that would happen in the future. Systems of writing, for example, are such *generic* and *modular* systems: the semantics of a given series of characters (that make up a word, for example) is not set in stone, but can fluidly morph to assume different meanings as time goes by, without affecting the *modularity and genericness* of the system of writing as such. We shall follow up the implications of *genericness* later on in Chapters 9 and 10.

8.2 THE PLATFORM CONCEPT AND THE ISSUE OF VIRTUAL WORLDS

An idea to technicize governance by means of online platforms to provide basic government services was published in 2010 by Tim O'Reilly, the founder of a well-known publishing house specializing in computer technology topics. In his essay *Government as a Platform*, O'Reilly (2010) suggested that governments should focus on providing basic digital infrastructure and services to maintain it, so that on top of this digital infrastructure citizens could exchange goods and services, as they do at a marketplace. Governments, he argued, should focus on providing further fundamental *platform services*, as they do in terms of a highway network, the police, fire services, garbage collection, etc., but this set of services should be adapted to new societal needs and technological advances to foster the economic prosperity of their users.

His idea was inspired by the evolution of the Web, which was based on cocreation of technology by developers from all over the world, as well as the Web's later evolution into a space in which consumers cocreated content through social media. What fascinated O'Reilly was the transformation of the Web from an infrastructure for the provision of digitalized content into a space in which informatization enabled the inclusion of new stakeholders. He called this new generation of the Web the *Web 2.0* (this term had appeared at the end of the 1990s (DiNucci, 1999)). O'Reilly became widely credited as the one who turned "Web 2.0" into a buzz (Graham, 2005) through his *Web 2.0 Summit/Conference* series in San Francisco that ran between 2004 and 2011.

The "2.0," as O'Reilly used it, denotes a renaissance period of the Web after the burst of the dot-com bubble at the turn of the millennium. It also reflects a shift from *digitalized* Web applications to *informatized* systems. Web 2.0 applications such as the Google search engine, the Amazon and eBay on-line markets, Wikipedia, or Facebook all utilize the new paradigm in which the users of the Web actively cocreate the services, rather than just passively consume information. What Wikipedia, Facebook, or Amazon provide are platforms on top of which their users can provide their own content, products, or services. This is the same paradigm as applied in the marketplace—there are market providers who offer a platform with the basic infrastructure and it is then the sellers on the market who provide the goods.

As such, these platforms have been designed as environments that invite coproduction. The success of any platform is simply determined by the success of the services and products built on top of it, as the success of a shopping mall is determined by the quality of the shops within:

> *It was not IBM but Dank Bricklin and Bob Frankston (VisiCalc), Mitch Kapor (Lotus 1-2-3-) and Bill Gates who developed the 'killer applications' that made IBM personal computers such a success. It was Tim Berners-Lee, not Vint Cerf and Bob Kahn (the designers of the Internet's TCP/IP protocol), who developed the Internet's own first killer application, the World Wide Web. And it was Larry Page and Sergey Brin, not Tim Berners-Lee, who figured out how to turn the World Wide Web into a tool that revolutionized business.*
>
> ***(O'Reilly, 2010, p. 29)***

Informatizing governance is exactly about this: it is about finding and engineering a platform that would facilitate the provision of governance in such way that the respective sovereign is able to steer it by means of technology. O'Reilly (2010, p. 12) called for something similar, namely "government stripped down to its core, rediscovered and reimagined as if for the first time." Alas, O'Reilly's *Government as a Platform* did not go any further than postulating a desired functionality of digitalized government, and simply remained on the level of marketing slang, a call for action to politics, and an advocacy of open government data (see Section 2.1.4 for details). His idea failed to provide a blueprint for its implementation and merely contributed to nurturing the myths and hypes associated with digitalizing governance, instead of *rediscovering and reimagining* government.

8.2.1 The Platform Concept in IT

The concept of a platform is indeed a very important one in informatics. *Platforms* in computer science and IT are fundamental sets of technologies that provide a basis on top of which other technologies can be built, or computer applications can run. Without platforms, modern IT tools could not be engineered. Accordingly, platforms are systems designed with *extension* in mind, which means that they provide a base infrastructure on top of which other software can exist.

The operating system of the computer (e.g., OSX or Windows) is one such *platform*. The programs which run on top of this platform (e.g., Word, Firefox, or Photoshop) all use the platform's functionality, which provides a whole set of basic functions, such as the visual rendering of the program on the user's screen, file handling (opening, saving), printing, keyboard and mouse operations, time and date, Internet connectivity, and user management. All this means is that the software developers do not need to occupy themselves with writing code that fulfills these basic tasks, as the *platform* provides standard interfaces that these applications can connect with.

There are a multitude of such platforms in the world of computers and informatics. For example, the operating system itself runs on top of an underlying, more rudimental, system which provides a platform for interaction with the hardware of the computer. Today, this platform corresponds to the specifications of the UEFI, the *Unified Extensible Firmware Interface*. From the 1970s until the first decade of the 21st century, one such base platform was the BIOS, the *Basic Input-Output System*, which provided communication between the computer hardware and the operating system. The operating system of the computer uses this underlying rudimental system for interacting with the hardware by making calls to standardized functions of the BIOS or UEFI interface.

Another example of a platform in the context of informatics is *Java*, a platform and programming language, one of the most commonly used and taught programming languages today, and the platform that powers the *Android* smart phones. Java is a bundle of technologies which include the Java programming language, the Java virtual machine (JVM), and tools and algorithms that translate (compile) Java source code (written by the developer) into code that is executed by the JVM. The JVM runs on top of the operating systems, which makes it possible for the same Java program to be run in Windows, OSX, or Linux without modification. To run an app on an Android smartphone, a complex set of platforms are stacked on top of each other to provide the user experience: the app itself runs in the JVM and the JVM runs on the Android operating system, which in turn runs on the Linux kernel that handles the interaction with the hardware components.

This layered stacking of platforms on top of each other is intrinsic to the culture of software, and has given rise to incredible innovation.

8.2.2 Virtual Worlds and Virtual Societies

One particular category of platform are the virtual worlds in participative computer games, the so-called *massive multiplayer online role-playing games* (MMORPGs). In these games, huge numbers of players from all over the world simultaneously engage in playing in the same environment, where they collect and trade items, groom their environment, and interact with each other within a virtual society.

These games come surprisingly close to a perfectly informatized economic and political society. Just like in the real world, inhabitants can have capital, do trade, have social and legal statuses, and enjoy their rights in accordance with rules provided by the sovereign. In fact, these virtual societies have their own internal economies of real-world significance, actualized through in-app sales. In 2003, for example, the size of the economy of *Norrath*—the virtual world inside Sony's game *Everquest*, was larger than the economy of Bulgaria (Lastowka and Hunter, 2004, p. 49), an EU member country of over seven million inhabitants. The scale of this economy is impressive—on average, professional players earned $3.42 per effective hour of gameplay (more than many laborers in India or China would have earned) (Lastowka and Hunter, 2004, p. 49).

From a technical perspective, each MMORPG is an IT system that resides on the game provider's server and with which players interact through specific graphic user interfaces that render to them the experience of the game. The gaming process involves a permanent exchange of electronic requests and responses between the player and the server, through which the player manipulates their jural relations toward the society and the other players with their character's legal status and other data relevant for the gameplay (e.g., position and appearance). Virtual real estate and other valuables are mere entries in the system's database, and trading between characters is nothing more than changing stored information.

Nonetheless, the way in which the players perceive these *bits and bytes* can create in them a sense of genuine possession and property and demonstrates how interactions in cyberspace can have tangible real-world effects. Dibbel (1998) reports of a dispute in the virtual world of LambdaMOO, a text-based virtual reality. Two neighbors, Martha and Dank, engaged in a nasty and protracted battle over Dank's dog being repeatedly poisoned and killed by the flowers Martha grew in her garden. Though it is not reported how that dispute was resolved, it is reported that both parties invested in the dispute the kind of passion and righteous indignation usually reserved for real-world across-the-fence property disputes.

It is not only the emotions and the money that can be real in these virtual worlds, but also the law. Both MMORPGs and real-world legal systems deal with abstractions of the real world. Accordingly, both systems can be seen as virtual constructs that provide a platform for managing rights and for ensuring systems of (legal) protection. While in the real world legal protection will predominantly be exercised by means of a complex system of institutions (courts, prosecutors, lawyers, police, prisons, monetary controls, etc.), the virtual worlds are governed by their architecture.

However, in contrast to the institutions of the real world, which themselves are governed by law and politics, the architecture of virtual worlds comes as is, and is not subject to politics and democratic discourse. Instead, the rules which govern virtual worlds are, as are the rules of technical platforms in general, hard-coded in an absolute, god-like, way.

This is not to say that politics cannot exist in virtual worlds. To the contrary, another example from Dibbels' (1998) *My Tiny Life* recounts the story of LambdaMOO's shift to democracy. After a virtual crime occurred—a character of a member of the community virtually raped two female characters by forcing them into committing virtual sexual acts against their will—the other members called for justice. Some called the *gods* (the "Wizards") to sanction the rapist, and for the establishment of a system of law, while others called for democracy. The community failed to reach a consensus, which was required to make the Wizards act. The Wizards—superusers with administrative privileges and access to the game's rules—refused to intervene in the gameplay, as it was up to the community to organize themselves because that was what the game was all about. The rapist then disappeared. What followed next was that the Wizards, without the consensus of the community, introduced politics and democracy. From then on, "any matter could be decided by ballot, and any proposition receiving at least twice as many votes for as against would become the law" (Lessig, 2006, p. 101).

We can debate whether or not what happened here was really a democracy. There are arguments that could support such a claim; *democracy*, after all, is a chameleon term of the political discourse that people can use to mean almost anything they want. What the LambdaMOO community got was a tool to change their platform, i.e., the architecture of the platform, and a tool to call for government interventions. While it was a self-governed community based on consensus, it had become a community governed not only by the architecture, but also by the Wizards, i.e., its "gods."

8.3 CONCLUSION

Both of these ideas—the reliance on *semantic* technologies or the building of a platform—are low-hanging-fruit. They share common problems: they both limit the possibilities to a discrete number of possible interactions and possible transmutations of the society. Reliance on semantics makes sense when it comes to modeling societies for the purposes of laboratory simulations, but is of no use in informatizing governance. This is not to say that semantics are of no relevance—their importance is explored in Chapter 10.

The concept of the platform per se is valid and useful in principle. A platform that does not rely on god-like administrators and that would offer unlimited, rather than a discrete, number of possibilities to interact with it would be viable for governance informatization. O'Reilly's idea of the *government* as a platform is jeopardized when there are hard-coded regulations that limit the possible ways of interaction with the platform. Hard-coding rules into a system is feasible as long as it can be assumed that no significant harm could be caused once such a system expires. Sustainability is no issue in MMORPGs—after all, they are mere games that will be played for a couple of years and then replaced by a new version—gamers know and expect that.

If "gods" were required to change the code of a technical system that governed real-world societies, it would defy the entire idea of governance informatization. Such a problem does not exist in MMORPGs, as the "gods" are the only government and sole providers of the platform of the virtual society. It is this very platform which confines the actions and possibilities of the society to the limited set of options made available by the mercy of the "gods." Even if a political forum could be established, as was done in LambdaMOO, this forum still relies on the mediation by external agents who control the system.

An idea that surfaces is to join semantic technologies with the concept of the platform and build an artificial language (e.g., a programming language) to describe laws in the form of algorithms. Kowalski (1992) did something similar by building an experimental system for automating decision-making in the context of British immigration law. Leibnitz' vision of a *Characteristica Universalis*, a mathematical system to calculate societal relations, was an idea that, had he succeeded, would have been this kind of artificial language. Even though such hypothetical artificial languages could allow for complex reasoning, their sustainability would be constrained by both the limited number of discrete semantics and the reliance on a "god" to continually update these to their newest version.

This problem can be nicely explained using Lego: Over 8700 different Lego elements have been produced (Eaton, 2016), such as the classic bricks, roof tiles, figures, horses and other animal figures, flowers, windows, doors, and mail boxes. All these elements provide a universe of interoperable toys, more than enough to keep a child busy till they grow up and beyond. But even if 8703 different Lego elements are available to model toy worlds with, one still will find that they're missing the 8704th element, and the 8705th, and so forth. Plasticine, on the other hand, allows the modeling of *any* environment imaginable without regard to scale, time, or fashion.

Thus, to *informatize* governance, a timeless and nondeterministic system, like Plasticine, must be found, rather than one rich in modules and options like the Lego system. This would prevent the crucial dependency on some omnipresent "god," to be the only one in the position to control the elements available in their paradise. As a core feature, such a system *must* be able to serve *any* society that has ever existed, and be able to serve any that ever could exist. This system should not be dictating constraints with regard to the society's power building processes, decision-making rituals, constellation of public apparatus agents, or any other characteristics of the public apparatus.

REFERENCES

Cerar, M., 1996. Večrazsežnost človekovih pravic in dolžnosti [Multidimensionality of Human Rights and Obligations]. Znanstveno in publicistično središče, Ljubljana.

Dibbell, J., 1998. My Tiny Life: Crime and Passion in a Virtual World, first ed. Holt, New York.

DiNucci, D., 1999. Fragmented Future. Print Mag. 53 (32), 221–222.

Eaton, D., 2016. How Many Types of LEGO Bricks/Parts Are There? [WWW Document]. Quora. https://www.quora.com/How-many-types-of-LEGO-bricks-parts-are-there. (Accessed 2 March 2016).

Graham, P., 2005. Web 2.0 [WWW Document]. http://www.paulgraham.com/web20.html. (Accessed 10 June 2019).

Hohfeld, W.N., 1920. Fundamental Legal Conceptions as Applied in Judicial Reasoning: And Other Legal Essays. Yale University Press, New Haven.

Jellinek, G., 1905. System der subjektiven öffentlichen Rechte [System of subjective public rights]. JCB Mohr (P. Siebeck).

Khazan, A., 2016. "Smart" in British and American English: A Comparative Lexical Corpora-Based Analysis. Università Degli Studi di Torino, Torino, Italy.

Kowalski, R., 1992. Legislation as logic programs. In: Comyn, G., Fuchs, N., Ratcliffe, M. (Eds.), Logic Programming in Action. Lecture Notes in Computer Science. Springer, Berlin/Heidelberg, pp. 203–230.

Lastowka, F.G., Hunter, D., 2004. The laws of the virtual worlds. Calif. Law. Rev. 92, 1.

Lessig, L., 2006. Code 2.0. Basic Books, New York.

Nora, S., Minc, A., 1980. The Computerization of Society: A Report to the President of France, pr. ed. vol. 2. MIT Press, Cambridge, MA.

O'Reilly, T., 2010. Government as a platform. In: Lathrop, D., Ruma, L. (Eds.), Open Government—Collaboration, Transparency, and Participation in Practice, pp. 11–39.

Peters, B., 2016. How Not to Network a Nation: The Uneasy History of the Soviet Internet. The Information Policy. MIT Press, Cambridge, MA.

Sharifian, F., 2007. Politics and/of translation: case studies between Persian and English. J. Intercult. Stud. 28, 413–424. https://doi.org/10.1080/07256860701591235.

Vitvar, T., Peristeras, V., Tarabanis, K., 2010. Semantic technologies for E-Government: an overview. In: Vitvar, T., Peristeras, V., Tarabanis, K. (Eds.), Semantic Technologies for E-Government. Springer, Berlin, Heidelberg, pp. 1–22.

CHAPTER 9

Nonmediated Governance

Contents

The previous chapter touched upon the issue of virtual worlds in the context of massive multiplayer online role-playing games. These games manage to provide an experience of informatized societies, as they are examples of societies in which the relations between their members are perfectly informatized. This perfect informatization has clear advantages—there are no conflicts in the relation between the subjects and the sovereign, no cases of administrative corruption, no courts to settle disputes between subjects, no law enforcement agencies, etc. That sounds pretty much like a perfect society, or does it?

The virtual worlds of online games are perfect *gardens of Eden*, paradises created by the "gods," who are the software developers and owners of the game. These "gods" created the environment in which the game takes place, they made the rules, and they roll out the updates whenever they please. All that is left for the subjects of the virtual worlds to do is enjoy the game and pray to the "gods" through online fora and helpdesk support. In these *gardens of Eden*, the constraints of all interactions are imposed top-down in an absolute way. The users of the system have little to zero influence on the extent or quality of the virtual jural relations with which they engage within the virtual world. The "gods" of the game may well permit users to design their own characters, influence the geography of the environment by adding virtual buildings, etc. Perhaps, the "gods" might even permit users to deliberate and vote on future features of the environments that might be implemented at a later stage. However, there is no other space for cocreation than that.

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00009-1

Such online games are genuine informatized societies, with a massive economy driving their existence; a system of subjective public rights which determine one's status within the game; and a system of governance, which is based exclusively on governing by architecture—the *code* of the game. Even the elements *subject-rights-sovereign*, which the *social contract theory* provides to model society, are perfectly reflected in these virtual worlds. The subjects (the players' characters) engage in virtual *public-right* type of relationships with the technical system (the sovereign). The system can grant them upgrades of their Jellinekian *legal status* or downgrade it, which then determines their ability to possess certain goods (e.g., weapons, armor, and vehicles) or to assume otherwise unavailable abilities. All of these options remain part of the hard-coded rules of the system itself, provided and controlled by the "gods" who created the system and who administrate it.

In contrast to these *gardens of Eden* that are the virtual worlds, real-world societies are not based on a *god-like creator* who is able to autocratically impose rules. Instead, real-world societies tend to self-organize and self-manage their own concerns. The systems and conventions that govern real-world societies, such as law and morals, change as time goes on and fluidly morph to adapt to the opportunities and constraints of their respective era. Real societies will morph from one political system to another, networks of power will rise and fall, economic opportunities will appear and disappear, the sovereign will at times be embodied in a single person, at times in a family, at times in a clique, and at other times in a class of people, a subset of the members of a community, a subset of inhabitants of a logical domain, and so on.

Chapter 8 dealt with three "low-hanging fruit" ideas from informatics on how governance could be informatized:

(a) to engineer a network of semantic jural relations based on the scaffolding provided by Jellinek and Hohfeld
(b) to build a platform on top of which governance would perform
(c) to engineer an artificial language to build governance rules and provisions.

The first option (a semantic network) was dismissed, as such a network could not sustain future changes to the underlying semantics and the change to their jural implications. Hard-coding *explicit* relations is an ill-advised idea in general, as it is not realistic to keep all global network of relations synchronized. (Think of the broken links on the Web alone!) The conclusion was that the sought-after *infrastructure* (we may well call it a *platform*) must be indifferent to concrete semantic constraints, i.e., it must be *generic*.

The second option (the platform of services) was dismissed as platforms suffer from the issue of a *god system* and limit the available options. And we do not want a *garden of Eden* here, since we already know that humanity is simply not mature to adhere to *god's* will in the long run. The conclusion from this, however, is not to avoid the *platform* concept as such, but rather to avoid the super-entity that controls the rules and the functions that such a platform provides.

The third option (the artificial language) would be a conceptual merger of both the predefined semantics and the *garden of Eden*, and, with regard to their flaws, is likewise not a solution.

The primary objective in the search for a system/infrastructure/platform for informatizing governance is to yield a system that is *timeless* (in terms that it could serve for millennia) and independent of the addressed culture (so that it can serve *all* cultures), i.e., *generic*. This must not be misunderstood for the *instantiation* of a system that would perhaps survive centuries, but rather a timeless and generic *model* of such a system. Take the case of a wheel as a model of a system that consists of a circular component that rotates on an axle bearing. Known instantiations of this model date back thousands of years, and new instantiations of this model are in use today. The timelessness and nondeterministic nature (genericness) of the wheel allow it not only to survive through the known history of human civilization, but also to be used for a variety of purposes such as wheels on the carriage, the potter's wheel, ship's wheel, steering wheel, cogwheel, waterwheel, and flying wheel.

Aside from merely being *generic* and *timeless*, the sought-after model for governance informatization must be able to function without any human mediation whatsoever, i.e., it must be *noninterpreted* and *nonmediated*. These four requirements boil down to a system of rules which govern a society's subjective public rights through its architecture (this then makes it *nonmediated*), whereby it must be able to change these rules without human intermediary agents who would need to interpret and translate the changes, as the Wizards of LambdaMOO did (see Section 8.2.2). This system of rules must then be able to accept any rule whatsoever, without verifying or questioning it, for it to be *generic*, which in turn disqualifies the application of artificial intelligence to govern society.

This chapter is a search for such a *model* of a system which would feature these characteristics. Section 9.1 recounts the first real-world attempt to introduce such a system into a real society, and the lessons learned. Section 9.2 discusses how *eligibilities* (i.e., Jellinek's *legally relevant allowed behavior*) can be *determined* rather than *described*, in order to address the issue with the explicit relations as dismissed in the context of semantic networks. Section 9.3 presents a toolset for describing and communicating the rules from Section 9.2.

9.1 ŠOFIŠ: PIONEERING NONMEDIATED GOVERNANCE

The first documented instance of a society that abided by the principles of nonmediated governance was established in Novo mesto, Slovenia, in April 2010. This was the *Student Union of the Faculty of Information Studies* (ŠOFIŠ), which we touched upon in Section 3.5.1, in the context of Liquid Democracy.

In Slovenia, the student unions are regulated by a lax law that gives high autonomy to student unions, as well as access to public funding that circumvents the state budget. As a result, established student unions are organizations with significant capital, which is, once in a while, subject to violent quarrels, during which students take sides either for the government of the student union or its opposition (Paulin, 2007). In order to prevent such violence from occurring at ŠOFIŠ, and in order to provide students with a novel platform for hands-on research, the organization established the separation of legal representation from disposal of capital and decision-making. Decision-making was limited to approving applications for funding of projects or changes in political appointments (whose existence was imposed by law). Deliberations were to take place outside of the information system and no decisions on the policy-level were possible.

The system of ŠOFIŠ was deliberately not about creating policies according to which the organization would work, but simply about regulating access to the treasury. To gain access to the treasury to fund a project, a member would have had to apply for the budget, providing a description of the project and the requested amount. The application would have been posted to a virtual billboard, in order for other members to vote on it using Liquid Democracy. Once an application had been accepted, the grantee would be granted access to make transfers from ŠOFIŠ' bank account up to the granted value of the project. The connection to the bank was engineered through an application programming interface (API) to the SWIFT banking network between the ŠOFIŠ information system and the German Commerzbank, which at that time was one of the rare European banks that provided this functionality to its customers. The entire transaction from the request for funding up to its use after democratic legitimization was thus routed through the information system, which enabled full transparency of actions.

Also prevention of misuse was deliberately not part of the system. If anyone had misused a granted project to embezzle funds, legal and moral prosecution would have to take place elsewhere. Thus, whom to trust and to what extent to trust was solely up to the society to decide by itself.

Each action taken would have been signed digitally using the qualified electronic signature. This included all actions of collaborative decision-making (voting), applying for a budget, applying for a political position or its recall, delegation of a vote within the Liquid Democracy system, etc. Any communication with the outside world, such as the tax return or the registration of the change of the legal representative, would have been conducted automatically by the system using templates. Furthermore, access to the e-mail account and digital signature of the organization itself would have been technicized in such way that at the very moment in which a change of the legal representative would have occurred, all access permissions would swap from the old to the new one.

ŠOFIŠ deliberately omitted any *nontechnicizable* features of government from its system, such as political culture, policies, or supervision. All these features would require a human interpretation of what is right, what is desired, or what is proper, which would then have potential for misuse of interpretative power. Only access to the most basic asset of the organization was regulated: money. Nontechnicizable features in relation to this asset could then still form and change over time. Ideas would have emerged about what is right and what is wrong, how money *should* be spent, and how this spending should be supervised, and so on. Policies on such matters within the organization would have fortified and changed over time. However, these should be of no concern to the *platform*, which should merely provide equal access to those who are eligible to it.

At the end of the day, ŠOFIŠ' information system informatized three core functions of the student union: the organization's budget distribution, its outbound representation (i.e., the presidency), and its internal decision-making processes. The system was largely constrained by requirements imposed from the outside, such as the requirement to have a representative at all, the technical link to the bank, and legal constraints with regard to scale and transformation. All of these contributed to the final design of the system, which was developed as an online platform that was hosted and managed by a *god-like* administrator.

Accordingly, though the governance of the student union was informatized as much as possible in the given context, the members of the organization were unable to access the underlying code in order to change it.

Members of ŠOFIŠ were restricted to collective decision-making about projects the student union would undertake and how it would use its resources. They could change the individuals in charge and the membership in the political bodies of the society. However, they could not change the system of collective decision-making or the set of political bodies of ŠOFIŠ. Their autonomy was constrained to controlling access to those resources they had from the start (e-mail account, bank account, organization's electronic signature) and had no option to add new informatized resources to this collection, such as access to the Web server or access to the office.

9.2 DETERMINING ELIGIBILITIES

Section 7.3 addressed the question: how can governance be informatized? On a conceptual level, the answer to this question was found in informatizing the jural relations and jural statuses into cyberspace, from where they could be controlled, changed, and so on. These jural relations contained information about the amount of Jellinekian *legally relevant allowed behaviors* that an individual could exercise in a given situation. A particular recipe of how to technically accomplish such informatization of governance has not been provided yet. The instinctive idea to go and explicitly describe legally relevant allowed behavior by means of semantic technologies was discussed in Chapter 8. However, any discussed options for explicitly storing jural relations were dismissed as technically unfeasible.

In order to informatize governance in ŠOFIŠ, a different approach was taken. Governance informatization was achieved by informatizing the seat of the president and other bodies of the student union, the communal budget, and access to the electronic signature. These informatized features of the organization allowed the members of ŠOFIŠ to govern access to them from within cyberspace. Instead of explicitly *describing* (in a technical way) eligibilities of individual members, for example, their right to access the communal budget and the organization's electronic signature, these eligibilities were *determined* from the informatized data ad hoc.

The method of *describing* eligibilities is about making statements such as "Paul is president; hence, he is allowed to command the community budget, and thus, he is allowed to pay the bill for the flyers." *Determining* eligibilities on the other hand is about asking questions such as "Is Paul eligible to pay a bill from the community budget?" Describing eligibilities implies explicitly regulating foreseeable situations in advance. Determining eligibilities on the other hand allows for reasoning in which the context cannot be foreseen. On the atomic level, the challenge amounts to informatizing jural eligibilities, whereby each eligibility can be determined by answering the question "Is person P eligible to action A in context C_T?," where C_T is the constantly evolving environment (hence "T" for time) and A is the desired status change of someone's jural status (e.g., the desire to become a mayor). We shall call this question the *PAC_T question*.

The *PAC_T question* can be applied to many situations, such as: Is Ann eligible to enter a theater performance? Is Carl eligible to receive his unemployment benefit for the previous month? Is Franck, the foreigner, eligible to enter a country? Is Lea, the law enforcement agent, eligible to take Rob, the robber, into custody? Is Marty the mayor eligible to pay for a new school building using public funds? Is the citizen council eligible to appoint Marty for mayor?

In ŠOFIŠ, the question "Is the requester eligible to do the desired action?" was asked each time access to funds was desired or each time one required access to the community's digital signature. This same question is asked each time a character in an online role-playing game aims to do an action, even if they had tried to walk through a wall. However, the query for the available permission in these cases does not take C_T into consideration, simply for the reason that there is no context. Context in itself is a variable, though it is part of the predetermined architecture.[1] Following is an example of what switching the context in reality means.

9.2.1 Morphing Context: The Cruise Ship Example

Let us imagine ourselves on a cruise ship. The ship offers boarding, security services, and entertainment, all dependent on the booked travel class. The passengers on this ship are a finite community that is bound to a specific territory (the ship) and are governed by the crew, who are responsible for upholding order during the trip and to provide the passengers with the contractually agreed-upon services. It is not a democratic government which governs this community (thus, the passengers have no ability to change the

[1] In a computer game, the character will find themselves traversing different predefined contexts—they might find themselves in the context of a virtual city, gliding through air attached to a parachute, or swimming in water. These, naturally, are different contexts, and the computer game will take this into consideration. It will do so by switching the set of rules that apply to the physics of the computer character and its attributes; it will trigger countdowns to determine how long the character can stay under water, and the like. However, all possible contexts of the game are already known in advance, which is why it is not *the* context that is switched, but rather a subcontext of the context of the game.

crew democratically), but it is a government nonetheless—they govern the passengers based on their privileges given by law.

This setting provides us with several avenues to explore jural relations between the government of this ship and its subjects, the passengers. The relation between crew and passengers is similar to the relation between a government and its subjects. The "social contract" in this miniature society is explicit and comprehensible: the crew is obligated to provide services to passengers on the basis of the traded set of rights, i.e., the purchased travel category. This setup enables us to conveniently calculate eligibilities on board, which are manifested in granted/denied access to services to passengers.

The mobility of the ship through national and international waters allows us to comprehensibly understand a change of legal context, as the ship may traverse multiple national jurisdictions that influence individuals' eligibilities, while the jural relations between crew and passengers remain unaltered. A change of one's subjective legal context can occur for many reasons, such as physically moving into a different legal context (entering a new country), or that a legal context extends into an area where one acts (such as the Third Reich's extension into Yugoslavia), or that a legal context morphs (as happened as part of the socialist revolution in Yugoslavia after the war). The reason why a legal context changes thus does not really matter.

Let us now consider a family (a father, mother, and their 13-year-old daughter who will turn 14 in two days) traveling second class from Piran (Slovenia) to Kish (Iran). The ship is expected to enter Iranian territorial waters on the fifth day of the journey. The ship features a wellness center, which has a swimming pool and a sauna. Entry to the swimming pool is included in the second class ticket, but not to the sauna, which is free only to first-class travelers. Entry to the sauna is not permitted to children under the age of 14. In Iranian territorial waters, Islamic law applies, which allows only single-sex usage of the sauna and one must be aged 20 or above to enter or accompanied by a close relative of the same sex.

In this example, we have a fixed community of subjects (the passengers) and a fixed government structure (the crew), but we have to deal with many dimensions: every member of this society has a status based on several relevant personal attributes, namely sex, age, cruise travel category, and relation to other travelers. This status entitles passengers to receive services and use the facilities. One attribute of the passengers—namely, their age—is subject to time, which is relevant, as the child—let's name her Eve—will become 14 and will thus become entitled to enter the sauna on the third day of the voyage. When the ship will enter Iranian territorial waters, the legal frame will change, which will also influence the passengers' legal situation, while their attributes will remain the same. Thus, on days 1–2, Eve must not enter the sauna, because she is to young; on days 3–4 she can go to the sauna, as she is now 14 already; from the fifth day on, she can go to the sauna only together with her mother, but not her father, due to the Iranian restrictions.

This example shows that the Hohfeldian *bundle of rights* or the Jellinekian *legally relevant allowed behavior* of each subject is determined by the context and the legal frame. If Eve tries to enter the sauna, then whoever controls this facility must grant or deny Eve access based on the available information about her age, family relations, and the information whether she has paid the entrance fee, as well as taking into consideration the then-valid legal context.

9.2.2 Constellation-Based Reasoning

The bundle of rights is not something that can be efficiently stored as a distinct piece of information, but must be interpreted every single time *based* on (i) the legal frame of the political community, (ii) data about the subject, and (iii) the context of the given situation. Let us define—inspired by Leibniz' appeal "*Calculemus!*"[2,3] the bundle of rights as B, the subject as S, the legal frame (L) of the political community P as L_P, and the legal context (C) of the particular request R (e.g., the request to enter the sauna) as C_R. We have data about each subject, d_S, and based on this data, we can calculate their legal status (ς) in the given legal frame:

$$\varsigma_S = \varsigma\left(L_P, d_S\right) \tag{9.1}$$

The legal status determines which bundle of rights somebody can have in a given legal frame, e.g., in a given country or other form of society. Thus, the bundle of rights of somebody in a foreign country is different from their bundle of rights in their home country. We can therefore say that both the subject's status (ς_S) and the legal frame (L_P) determine the subject's bundle of rights:

$$B_S = B\left(L_P, \varsigma_S\right) \tag{9.2}$$

[2] "*… quando orientur controversiae, non magis disputatione opus erit inter duos philosophos, quam inter duos computistas. Sufficiet enim calamos in manus sumere sedereque ad abacos, et sibi mutuo (accito si placet amico) dicere: c a l c u l e m u s*" (Gerhardt, 1890, p. 200).

[3] "*Wer kann was Dummes, wer was Kluges denken, das nicht die Vorwelt schon gedacht?*"—"*Who can think wise or stupid things at all that were not thought already in the past?*" (Goethe's Mephisto in: Jellinek, 1892, n. 18).

In order to determine if somebody is permitted to action R, we must first find the set of rights required to perform it. This set of rights or eligibilities (E) is determined by C—the context of the given request, which is dependent on the general legal frame (L_P). To calculate set E for a given action R, we perform:

$$E_R = E\left(C, R\right), \text{where } C \subset L_P \tag{9.3}$$

If we now want to find whether S has permission (Y) to a specific action R, then we must check whether the set of required rights/eligibilities to perform R is contained in its bundle of rights B:

$$\text{if } B_S \supset E_R \text{ then } Y_R \text{ is true, else false} \tag{9.4}$$

As we see, making governing decisions (based on finding Y_R) and thus governance as such depends on information available to the system (d_S). Thus, if the available information about Eve's age would be mistakenly stored as >20, then she could go to the sauna every day, despite the biological truth. Also, as her family travels second class, they must pay every time for their sauna visits, which they would not have to do if the stored information would be different.

A change of information regarding the legal status of a subject ς_S and data about the subject d_S available to the sovereign results in a different bundle of rights B_S. Therefore, in order to reach nonmediated governance, we need to be able to manipulate ς_S and d_S directly ourselves, or more precisely, we must be able to manipulate d_S, because the legal status (ς_S) is determined by the data, which is the only tangible variable independent of the legal frame (L_P).

In modern systems of governance, manipulation of d_S is performed by the bureaucratic machine. In order to change even the simplest data such as name, address, or marital status, we have to fill in forms and wait for applications to be processed.[4] The same is true if we want to receive child support, obtain permission to drive a car, or become owners of real estate. Bureaucratic decision-making (in terms of Weber's model), as well as digitalized decision-making in e-Gov, use a multiple-process-based approach to effectively determine Y_R. Through a series of partly autonomous processes (both customer-facing processes and internal business processes (cf. Leben and Vintar, 2003)), ς_S (e.g., adulthood) and d_S (e.g., name, date of birth,

[4]An attempt to tackle bureaucratic processes using semantic technologies was demonstrated, e.g., by Klischewski and Ukena (2010). As discussed in Section 8.1, however, resolving to semantic technologies would be unfeasible.

address of residency) are gathered and Y_R (e.g., the eligibility to change address/name/ownership of real estate) is determined.

In contrast to the traditional process-based approach, the method described above relies on states or *constellations* of data. This method deliberately rejects finding Y_R through a series of cascading processes and subprocesses, as each process takes valuable time and is vulnerable to errors. Instead, we propose the manipulation of d_S based on the ad hoc determination/calculation of Y_R—R being the permission to manipulate d_S—in one logical step.

Such *constellation-based reasoning* (CBR) functions like a key opening a pin-tumbler lock, where the key, due to its specific shape, moves the pins into the right constellation and allows the lock to be opened (Fig. 9.1). In the cruise-ship example above, the *lock* would be the specific constraints that govern the access to the sauna (age, sex, and whether or not the passenger has a valid ticket) in the given context; thus, Eve's *key* would be the constellation of the information available about her. In contrast to this, process-based determining of Y_R would be like a doorman in front of a nightclub who would decide about whom to let inside based on his own *interpretation* of the house rules.

In order to change the key, or the lock, without human translation, the model needs to deal with both read and write access to d_S (the collection of data available about the subject). To govern this access, we again can apply the *key:lock paradigm* of CBR, so that the stored constellations of data enable (or prevent) the access to reading or writing the data itself. The CBR's *key:lock paradigm* provides a closed-loop system in which the mechanism of rules (locks) used to govern access to the core data (d_S) is the same as the

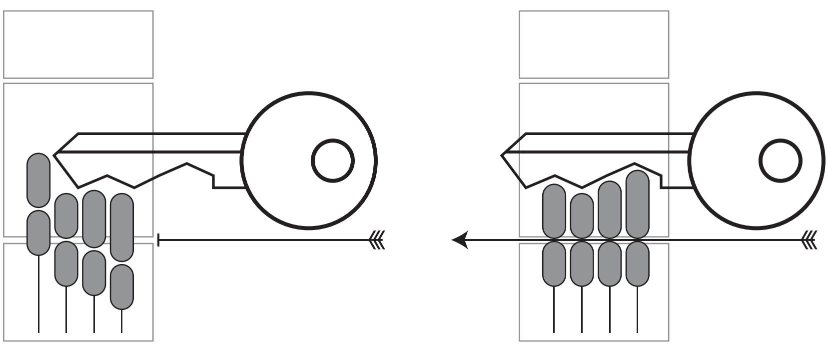

Fig. 9.1 ***Constellation-based reasoning is like a pin-tumbler lock.*** The pins are the conditions which the key (one's existing eligibilities) must satisfy in order to unlock the desired action (the arrow).

one which governs the defining of the rules. Accordingly, the rules can be reconfigured at runtime based on the then-valid rules, which in turn would change the access mechanism as such.

9.3 A TOOLSET FOR DESCRIBING RULES FOR CONSTELLATION-BASED REASONING

For describing systems of CBR rules we have developed a dedicated diagram technique, which provides the means to depict constellations of conditions/nonconditions that must be fulfilled in order to enable an eligibility.

Fig. 9.2 describes the CBR locks that regulate access to the sauna from the cruise-ship example in Section 9.2.1. The left part of the picture shows the CBR constellation that governs access to the sauna in Slovenia, where the only constraints are a valid ticket and age. The constraints imposed by the Iranian context are depicted on the right side of the picture.

This diagram technique can be used to visually describe/model rules in the form of constellations of data, which represent the pins of CBR's metaphorical "locks." These locks can be modeled by means of elements A–F, as depicted in Fig. 9.3. These elements are explained as follows.

[A] is an assertion about a subject in the form of context-relevant information, such as "this person has a valid job contract" or "this person has been born in 1984." Assertions such as these can be stored as raw data in a database, or they can be information that is the result of evaluating other CBR expressions. Contemporary examples of such raw data are the infor-

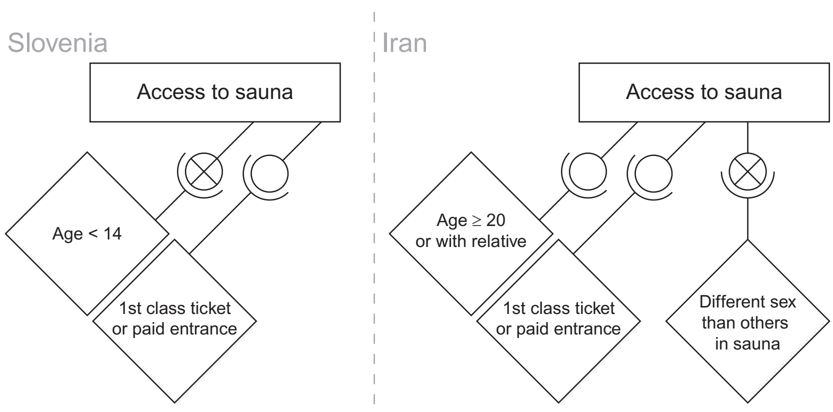

Fig. 9.2 ***Context-dependent CBR locks from the cruise-ship example in Section 9.2.1.*** *Left*: Slovenian CBR lock; *right*: Iranian CBR lock for the same eligibility, i.e., access to sauna.

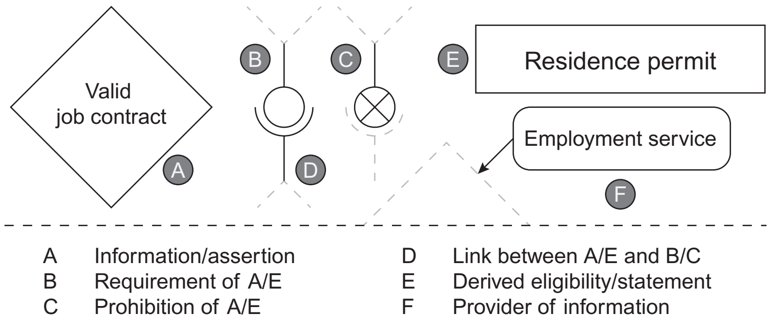

Fig. 9.3 Elements of the diagram technique to model constellation-based reasoning.

mation contained in the birth certificate or registration card. Examples of derived assertions are statements about one's employment status, the information whether or not a person has a criminal record, and so on, which again is based on other raw data. In practice, the raw data would be provided by agents that are legitimized to provide such data, for example, courts, registration offices, and parishes.

[B], **[C]**, and **[D]** are connecting elements, which make up the "pins" of the metaphorical CBR lock. As such, they define the conditions which need to be fulfilled by elements linked with [D] in order for the elements linked with [B] or [C] (assertions described by element [A] or constellations described by element [E]) to be valid. **[D]** is the neutral connector between an information [A] or [E] and an operator [B] or [C]. The operator **[B]** mandates that the south-bound element's condition must be *true*—e.g., mandates that a person must have been born in 1984. The operator **[C]** negates the condition—e.g., mandates that a person *must not* have been born in 1984.

[E] is the eligibility/statement that is the desired result of evaluating a CBR expression. In practice, this can take the form of a granted permit, granted access to a common resource, the affirmative determination of one's professional or political role in a given scenario, etc.

The labels in Fig. 9.3 are taken from the residence-permit scenario discussed in Section 1.3.4, in which an application for a residence permit took an unreasonably long time. Among others, the applicant in that scenario had to provide proof of a valid job contract—thus, a valid job contract was one of the elements of the constellation required in order to *unlock* the residence permit. While in the figure a *job contract* is depicted as an assertion, the job contract might as well be a *set* of tangible data. We may argue that a job contract is established once two subjects—the employer (usually its representative) and the employee—agree on certain minimum terms, such as the pay, the date of beginning, the number of work hours per week, and a job description. While it is likely not feasible that the fourth condition could be informatized, the other three conditions can easily be modeled in a structure that would describe an informatized contract. This demonstrates that the granularity of data stored in the system is not determined by the system itself, but rather it is up to the evolution of the system to define the semantics of the collected data and their application in the context.

This diagram technique allows for an abstract description of eligibilities in informatized nonmediated governance. Policy makers, system architects, and other parties involved in designing rules and eligibilities thus gain a toolset for analysis and communication. Pioneers of governance informatization can use these to rethink and reengineer contemporary administrative procedures, which yield the assertion of eligibilities in the form of documents and decrees, to transform them into constellations of informatized CBR locks and keys. In the context of an already informatized governance system, this technique can be used to plan and communicate legislative changes, and to document and visually express existing laws. Further advanced tools can then be developed, and could translate such visual diagrams into executable code, which would represent the rules that can be directly applied in technical systems that enable nonmediated governance.

REFERENCES

Gerhardt, C.J. (Ed.), 1890. Die philosophischen Schriften von Gottfried Wilhelm Leibniz [The philosophic works of Gottfried W. Leibniz]. Weidmannsche Buchhandlung.

Jellinek, G., 1892. System der subjektiven öffentlichen Rechte, Elibron Classics series 2006. Akademische Verlagsbuchhandlung von J.C.B. Mohr, Freiburg.

Klischewski, R., Ukena, S., 2010. E-government goes semantic web: how administrations can transform their information processes. In: Semantic Technologies for E-Government. Springer, pp. 99–125.

Leben, A., Vintar, M., 2003. Life-event approach: comparison between countries. In: Traunmüller, R. (Ed.), Electronic Government. Springer, Berlin, Heidelberg, pp. 434–437.

Paulin, A., 2007. Izgredi ŠOUM 2007 [The 2007 Riots in the Student Union of the University of Maribor]. Dvojka 1, 14–19.

CHAPTER 10

Model for Nonmediated Governance

Contents

Chapter 9 elaborated on how to manage the creation and determination of Jellinekian *subjective public rights* with no requirement for intermediate human mediation. To achieve this, *constellation-based reasoning* (CBR) was introduced as a mechanism to govern access to raw data, in order to derive a person's eligibilities in a given context. CBR can be thought of as a system of *locks* to restrict access to data and *keys* to unlock them.

These metaphorical keys are virtual constellations of known data in a given context. To unlock a metaphorical lock, the constellation of data must meet the terms mandated by the lock. By unlocking a lock, one can write new data to the context, change it, or delete existing data. By doing so, a person can, for example, change their address of residency in a database, enroll as a student in a university, or receive their monthly state pension. The locks would define the required composition and characteristics of the keys, which govern the circumstances of eligibility, for example, to receive state pension.

CBR is an essential prerequisite in defining a model of nonmediated governance (*nm-Gov*), in terms of a framework for creating, storing, retrieving,

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00010-8

and changing informatized assertions, based on which eligibilities of jural subjects can be determined. The objective of nm-Gov is to enable such interaction with the informatized assertions without human mediation, and without the need for interpretation of rules that govern the interaction. Rules that do not need to be interpreted by human intermediaries for effective application would allow a person's eligibilities in a given situation to be determined automatically by machines. In this capacity, CBR is an enabler for a technical governance system that does not require a *god-like* system administrator. As there would be no administrator acting as an obligatory passage point for changing the rules of how the system works, the rules by which a society is governed could morph fluidly as society evolves.

However, while CBR comes as an enabler for a sustainable base infrastructure to store and communicate jural data, it does not address the full complexity of the present design challenge. In order to design a technical system that brings a form of governance to life, with no human intermediaries to administer jural relations in the society, there are further challenges to be solved. A major challenge, for example, is the definition of the keys and locks. More specifically, if constellations of jural data enable eligibilities, then naturally one must ask how to recognize such constellations.

This brings back the need for the domain-specific semantics, as discussed in Chapter 8. The focus of the discussion there was on the feasibility of Semantic Web technologies to create a network of semantically interlinked jural relations between individuals. The feasibility of such an endeavor was dismissed, as such a network would be too complex to maintain. The focus in this chapter, on the other hand, is on the ability of semantic technologies to describe concrete constellations of data. This could be used to describe the data structure of a university degree, a driving permission, a land parcel, or a political representative's mandate. What is crucial here is that these data structures must remain independent from the infrastructure responsible for *creating, reading, updating, and deleting* (CRUD) the informatized assertions, in order to ensure the sustainability of the infrastructure.

At the end of the day, a real-world system that would enable nm-Gov needs to take into account many different aspects, some of which are less *timeless* and *generic* than others. To put these aspects into perspective, Section 10.1 presents a five-layered approach of how to structure nm-Gov for real-world use. Section 10.2 focuses on the *timeless and generic* components of this architecture, i.e., where the core data is stored, and discusses its jural and technical requirements. Section 10.3 provides an overview of how such a system would enable us to reconsider the roles of traditional governance agents. Section 10.4 concludes this chapter with a discussion.

10.1 THE CONCEPTUAL STACK

How can *nm-Gov* be established by means of ICT? Expressed through a conceptual stack, nm-Gov may be seen as an architecture comprising five layers, as depicted in Fig. 10.1.

10.1.1 Layer One: Communication Network

The first, bottom-most layer is a technical communication network, e.g., (though not necessarily) the Internet. This layer is about exchanging arbitrary messages by means of telecommunication. Any evolution of this layer must not have significant implications on the next, just as the introduction of the Internet or the introduction of mobile communications had any implications on the fax machine.

For example, while the only mature technology today is electronics-based computing and telecommunication technologies, research from physics suggests a future in which quantum technologies are expected to yield a new generation of infrastructure for secure and fast communication (de Touzalin et al., 2016). Crucial building blocks for quantum networks, such as quantum repeaters and quantum processors, have been already successfully demonstrated on a proof-of-concept level (Duan et al., 2001; Liao et al., 2018; Ma et al., 2012; Villoresi et al., 2008; Yuan et al., 2008). Accordingly, a transfer from electronics-based telecommunications, data storage, and data

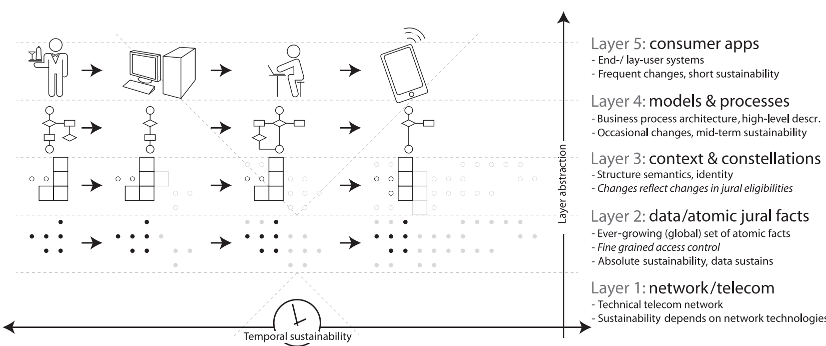

Fig. 10.1 ***Five layers of nm-Gov.*** Layer two, where the data is stored, is per definition timeless and generic.

processing to quantum technologies in a distant future would change the way data is stored and communicated at this layer.

10.1.2 Layer Two: Assertions and Access Control

The second layer is about a "content-agnostic" technical infrastructure that enables arbitrary communication and manipulation of informatized assertions and core data. Accordingly, in this logical layer, the data is stored, whereby the access to this data is governed by means of a mechanism such as the CBR (Section 9.2). In principle, the data stored in this layer should be able to remain there forever. Even if the underlying infrastructure in layer one, to physically store and exchange the data, changes to a new generation of technology, the data in layer two would remain. (Likewise, when solid state drives succeeded magnetic hard disk drives, the data they stored was not affected.)

The mechanism for governing access to the informatized assertions must be content-agnostic, in terms of that it only blindly applies the rules (as defined in layer three) to the incoming requests and responds in accordance with these rules. The model of such a mechanism can in principle remain the same forever, just as the wheel-and-axle principle has remained valid.

10.1.3 Layer Three: Context and Semantics

The third layer is about contextualization, in terms of providing artifacts that would define domain-specific data structures, semantic conventions, *identity*, etc. This layer would enable interoperability between nodes that would constitute the network defined in layer two and provide the corresponding semantics. Querying this layer would provide answers to questions such as whether or not one is eligible to their state pension. In this layer, the structure and semantics of constellations that, for example, denote a land parcel, a university degree, or a diplomat's jural status would be stored in the form of CBR locks and keys.

A clear separation of the third layer from the second is crucial, as the semantics and structures of layer three will change over time. For example, to *have* a university degree, the requirements tomorrow could be slightly different compared with the requirements today or yesterday; nonetheless, the *complex concept* of a university degree, which entitles individuals to certain eligibilities (e.g., only individuals with a university degree are permitted to compete for certain civil service jobs), may survive many changes in its intrinsic composition, perhaps until some point in the future when this concept loses its original value.

An example of such a *complex concept* which has become obsolete over time are the aristocratic titles of the Austro-Hungarian monarchy—in the past, they *enabled* access to government jobs, though this function was lost after the sudden dissolution of the monarchy. Nevertheless, the system of titles still remains in use, even though no formal value is associated with them. A similar example is the scientific doctorate. Decades ago, having a doctorate entitled one to a tenure-track lectureship position, though now this progress has essentially become obsolete, such that young doctors of science even struggle to find short fixed-term contracts.

These *complex concepts* of the *contextualization layer* (layer three) are the *locks* in CBR, which are unlocked through the fulfillment of the required constellations of data as stored in layer two.

The contextualization layer could be established and governed by professional guilds, which would determine the proper definitions and the micro-architectures for complex jural concepts. For example, a guild of academic institutions could jointly define a de facto standard of what data structure a bachelor degree should have when stored as core data in layer two. This would enable a subject, who perhaps graduated from a British university, to enjoy the eligibilities associated with having tertiary education in Slovenia without the need for any additional homologation. The British university in this case would be the technical host of the jural facts from layer two and could be referred to in order to be utilized as a *key* (or part thereof) to *unlock* eligibilities in other legal domains.

10.1.4 Layer Four: Models and Processes

The fourth layer is about designing and documenting the various administrative processes one has to go through in order to unlock desired eligibilities. In the example of the residence permit from Section 1.3.4, the applicant had to undergo a process that involved obtaining assertions from various parties (language school, police, employment service) before a residence permit could be granted. This process could be modeled visually using the diagram technique described in Section 9.3.

In the context of nm-Gov, however, a "process" is not literally a process, as there is no predefined flow of steps that one must follow in order to arrive at a result. Instead, the result is achieved through a system consisting of multiple levels of hierarchically interdependent CBR locks, in which earlier unlocked locks present part of the key for later ones. For example, in order to be selected for a civil service job, one must have first applied for such a job, and in order to apply for such a job, one must have before fulfilled all the requirements for *having* an appropriate university degree.

Visually modeled constellations and processes can be used to communicate requirements of unlocking eligibilities to the public and professional audiences. Designers of end-user software and policy-makers can use these models to do their jobs, while the models can be publicly discussed, scrutinized, and optimized.

10.1.5 Layer Five: Applications

Finally, the fifth layer is about the technical artifacts that provide means for user-friendly interaction with the network of jural relations. This is the layer in which graphical user interfaces (GUIs) are set, as are the machine-to-machine interfaces, technologies for planning, visualizing, analyzing, etc. These artifacts enable advanced options for subjects and citizens to interact with the layer two data and the service providers of the public apparatus; these could either be developed in the form of user-friendly systems subsidized by the state or a local community or be commercial products that facilitate interaction with layer two data.

The careful reader will have noticed that layer five again brings us back to the level of today's e-Gov, i.e., it introduces consumer-level apps addressing citizen and business for interaction with the state. This is true for sure; however, there is a core difference between nm-Gov and e-Gov. The mistake of modern e-Gov was that it *began* by providing monolithic layer five artifacts. As discussed in Section 4.1, the approach taken in e-Gov resulted in artifacts which are not technically and functionally sustainable; they have issues with interoperability, violate core jural concepts such as the principle of legality, and cannot be democratically controlled. It would also not be wise to start design and development of a new system for technicized governance at layer four. Doing so would imply the description of business processes on a high level and then their automatic translation into the program logic of e-Gov artifacts. While this might work to satisfy acute needs (as e-Gov does), it will not be able to cater to an unforeseeable future, as is required by nm-Gov.

10.2 REQUIREMENTS OF THE ELECTRONIC REGISTRIES

The idea behind nm-Gov is that the agents of the public apparatus host a collection of registries containing data about their subjects, just as data is stored in the civil registry, cadaster, or business register. Based on these collections of data, one's specific legal status and bundle of rights can be determined/computed given the specific context or situation. These registers must be defined in electronic form and must be accessible remotely by means of ICT, e.g., through the Internet.

The electronic registries, however, must not be hidden or obscured from the subjects who are to use them. Hiding them would defy the main purpose of nm-Gov, as mediators would again be required to govern what is hidden and what is not hidden. As it is the registries that store the data based on which individual eligibilities are determined, certain factors of integrity must be assured. We can identify the following requirements to assure proper integrity of the registries:

1. The public interface to the system, i.e., the location of the interface in the network (e.g., URI), must be defined at the level of law.
2. The format of incoming and outgoing messages must be clearly standardized and binding at the level of law.
3. The procedure of handling any incoming request must be defined at the level of law.
4. Reading and writing data must be done in an "analogue" manner.
5. Legally binding and *fair nonrepudiable* (Section 12.3) communication between the sender and the server must be ensured.
6. Users must have full access to the core data within legally imposed restrictions.

Requirements 1–3 ensure that everybody can know where and how to reach the endpoint of the nm-Gov system, as well as how the request will be processed. Thus, the user is not bound to use specific terminal equipment or interface to interact with the system, but can hypothetically build terminal equipment for themselves. These requirements can be imposed through rigorous technical standards incorporated into the legal system.

The word *law* in requirement 1 is not to be interpreted as written law as we know it today. Rather, we use it to denote an equal level of legitimacy. It is conceivable that a *root registry* could be defined similarly to a modern-day constitution, for example. This *root registry* could then contain the information about the locations of other registries and define the constellations (*locks*) required for read/write access to this registry.

Requirement 4 implies that only the grammar and semantics for defining the commands for accessing data must be defined. *Analogue* here means that virtually any possible request (e.g., for reading, writing, updating, or deleting data) must be accepted by the system; such a request may contain a virtually unlimited number of conditions that influence the action of the receiving system. This requirement excludes, by definition, the possibility of using templates for regulating data access; instead, it implies the use of a structured language for reading and writing data.

Requirement 5 is essential for connecting and bringing data together from sources which are not originally linked. Let us imagine a private-sector bank which we trust to execute a payment to our business partner, provided that certain conditions are fulfilled—e.g., our business partner must first prove that they have transferred ownership of a real estate to us before we pay them the purchase price. The bank could provide an application to receive the information from the land registry, verify it, and then conduct the transaction. The bank must therefore be able to fully trust the integrity and correctness of the information. The receiving information system on the other hand must be able to be absolutely sure about the identity of the sender and the integrity of the request.

Requirement 6 gives the subjects maximal freedom in designing their jural relations in accordance with the surrounding legal frame. This freedom can enable the discovery and development of new ideas regarding the function and utility of governance. Some novel ideas in this regard will be discussed in Chapter 14.

10.3 STAKEHOLDERS AND ROLES

Online role-playing games (see Section 8.2.2) and other online societies, e.g., online markets, have two distinct stakeholders: the sovereign in the form of the corporation that operates the system and the subject, who is the player or the user of the system. Each interaction between the stakeholders is regulated by the system's architecture, the design of which is at the sole discretion of the provider and generally hidden from the public. The code of such platforms is simultaneously law, jurisdiction, public administration, and government.

Real-world societies, on the other hand, are based on rules subject to changes in the course of time. These rules have to be politically proposed and (e.g., democratically) legitimated, and should be transparent to all in order to conform to the principle of legality. These rules determine how jural relations are created and manipulated, and they define which information is needed for such actions.

Below we outline two ways of how to achieve either full *nm-Gov* or, as an alternative, how to gradually introduce nm-Gov into the existing bureaucratic culture in the form of a hybrid.

10.3.1 Pure nm-Gov with Liquid-Democratic Decision-Making

In the first mode, we assume a *blank-slate* society which decides to democratically govern themselves via nm-Gov with a minimum of human mediation. In this scenario, decisions about rules and regulations (the law), governmental registries, public spending, assignment of public mandates, etc., are made through Liquid Democracy (cf. Section 3.5.1).

Such a society would require the following stakeholder groups.

(i) Subjects

Each citizen is a subject that interacts with the nm-Gov system in order to propose and vote about new rules and registries, the access to public money, assigning mandates, etc. Subjects would interact with the nm-Gov system to influence their jural relations and jural statuses, to exercise their participative rights, to assume mandates, to request and receive public funding for their projects and public assignments, etc.

(ii) Agents

Agents are subjects to whom governmental mandates have been assigned, such as police officers, judges, examiners, and representatives of groups. Thus, they are subjects with an *active* legal status, who are obliged to enforce law and order and are the face of the sovereign.

(iii) Service providers

Service providers aid subjects in their interaction with the electronic registries by providing user-friendly access, such as interactive GUIs, agencies for human-mediated interaction (where subjects would interact through "human" interfaces similar to modern-day notaries and street-level civil servants), or application programming interfaces and programming libraries for developers.

In order to keep the technical systems up and running, a further class of subjects would be required—the administrators. They, however, would not be "gods," as in the case of virtual worlds (Section 8.2.2), but mere aids to the system.

(iv) Administrators

Another group of subjects with an *active* legal status would be technical administrators, who would take care of the maintenance of the technical infrastructure.

The nature of Liquid Democracy implies the possibility for hierarchical structures to emerge. Thus, the system does not aim to prevent a group of subjects from transitively organizing themselves to such an extent so as to enable a charismatic subject to rise to the position where they might request to be addressed by the public as a *leader/king/president/marshal/first citizen*/etc. This subject then might use the power transitively invested in them to define further positions of power to which they could appoint cabinet ministers, who would appoint their secretaries, who would appoint their officials, etc.

While this would mean that formal structures, as they exist today, could be remodeled, the whole system would remain based on a sustainable electronic foundation that would make it possible for such structures to be easily reshaped by collective will—political revolutions might be thus conducted without terror, bloodshed, and war.

10.3.2 Hybrid nm-Gov

As an alternative to the blank-slate implementation, a compromise can be found in a hybrid mode, where we assume that nm-Gov is to be introduced gradually into the existing political culture and structures. A society governed in hybrid mode will require, in addition to the roles defined in the blank-slate option described above, the following roles of subjects with active legal statuses (Fig. 10.2).

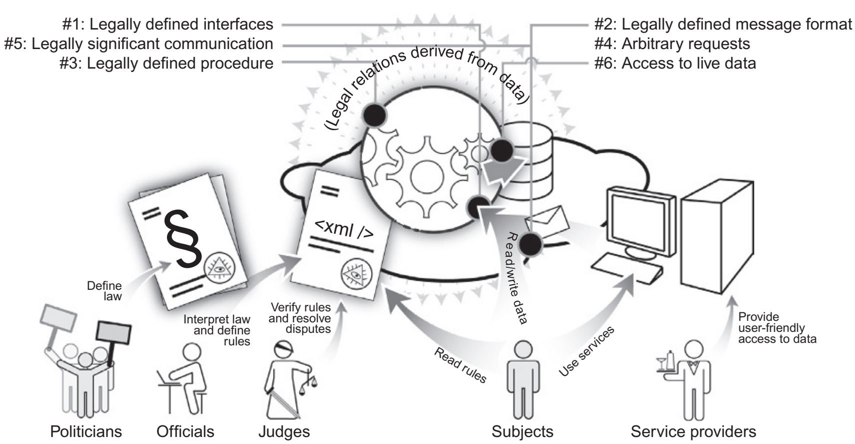

Fig. 10.2 Stakeholders of an nm-Gov system if introduced in hybrid mode.

(v) Politicians

Politicians are subjects who design descriptive policies on how the society should be regulated. These policies can also be laws or other kind of regulations. In the next step, these policies must be translated to a form that can be handled electronically.

(vi) Officials

Officials are people who have been charged with executing law and policies, which they do in nm-Gov by centrally defining the electronic registries and by defining the rules for their read/write access. Thus, their role remains similar to their role today, instead of e-Gov systems they now design nm-Gov registries.

As the gap between the descriptive rules and their electronic implementations is now bridged by human labor (which is not infallible), disputes could arise regarding the correctness of the implementation of law into the digital realm. To resolve such conflicts, dedicated judges are required.

(vii) Judges

In order to resolve such conflicts which might arise due to the official translation of policies into nm-Gov registries and rules, dedicated judges are required, who unlike today's judges must have profound knowledge of both law and informatics.

In the hybrid mode, the existing *trias politica* (the separation of the legislative, executive, and judicative branch) is maintained, including its personnel. However, the power of the modern civil service is divided between three roles—the *officials*, the *agents*, and the *service providers*. All of the interaction in this mode is moderated through the nm-Gov infrastructure.

10.4 SUMMARY AND DISCUSSION OF NM-GOV

In this chapter, we have developed the conceptual architecture and identified the stakeholders of *nm-Gov*, if applied in the real world. This section aims to provide a short overview and discussion of this model.

nm-Gov is based on the assumption that jural eligibilities can be determined from informatized data. While this assumption is not groundbreaking on its own—the reliance on (government) data to determine one's eligibilities is in wide spread use today—what nm-Gov introduces is a systemic approach to deal with that data.

When, for example, a member of parliament casts a vote, they can do so only because they are known to the respective democratic body as one who is eligible to act in this way. If one wants to transfer ownership of their land parcel to someone else, they will be able to do so only because the information on their ownership is known to the land registry. In all these cases, evidence has been generated at some point in time, from which it can be concluded with certainty whether or not somebody's actions are legitimate in a given context.

Thus, if the mayor of a town was about to sell real estate owned by the community, we might assume that he is eligible to do so, if we know that *(a)* the real estate truly is owned by the town, *(b)* the person conducting the transaction is truly the mayor, and *(c)* the transaction has been approved by the town council. Condition "*a*" can be satisfied by taking a look at the land registry.[1] For condition "*b*" to be true, the mayor must have been elected *(d)* by a majority of the voters participating in the elections; thus, to verify condition "*d*" we would have to count the popular votes in favor of the said candidate and verify that each of the votes was truly cast by a voter belonging to the constituency. Finally, to verify condition "*c*," we would have to investigate whether the legitimacy to sell the property was indeed given by the town council with a majority of its votes, though we might be tempted to investigate whether or not each of the council members themselves were properly elected by legitimate people, etc.

The point here is that all legitimacy can be brought down to verifiable facts, such as the collection of cast votes by the group of eligible voters. Personal preferences (such as votes) cannot be further divided and must be stored as *assertions*; the same applies to professional verdicts, such as a student's grade given by a professor or court rulings. Based on these assertions, eligibilities can be determined, such as a student's eligibility to advance to the next level or a land owner's eligibility to request assistance in demolishing an unlawfully built building on his land.

Guaranteeing the conditions *a*–*d* from the above example in mediated governance (i.e., what we have today) would be the responsibility of various committees, each of which would compose a report and issue a

[1] In most continental-law countries, the land registry is a trustworthy source of information about the legal status of real estate. We might trust that the real estate's owner is the person indicated in the land registry. An exception to this rule was introduced in Slovenia with the *Denationalization Act* of 1991, which regulates the restitution of property that was nationalized after the socialist revolution during the World War II. We touched upon the issues that followed in Section 1.3.5.

verdict/assertion. The work of these committees would be vulnerable to clientelism and other forms of corruption, as they could easily become a target of accusations of misconduct, which in turn might trigger protracted political and legal battles, and so on. On the other hand, in nm-Gov all these conditions could be assured by means of technical rules, and all actions could be routed through the technical infrastructure of the nm-Gov system. Casting a vote would technically result in writing a new data entry into a database. This write access would be possible only if the requester (the voter) is eligible to do so, which then would be determined based on informatized data already stored in the system. Accordingly, the mandate of mayor would be based on clear mathematics instead of assertions of mistakable committees, etc.

But what about law? Does law not properly regulate how officials must behave? Would this not already guarantee that the committee members, who solemnly swore that everything is fine and proper, were not the finest, most trustworthy, and independent individuals? And would law not step in if there was something about to go wrong? Alas, law does not protect. Rather, it merely provides legitimacy to call upon state institutions for protection. Then again, neither do institutions protect. They merely provide a framework for legitimate requests to call upon individuals, who committed themselves to use their function's legitimations in order to act as law mandates, etc.

The modern public apparatus, despite all of its regulations and legal frameworks and all of the institutions and titles, is ultimately nothing more than a system of individuals who draw their legitimacy from data, affording them their honors, their salary, and their rubber stamps. This data can easily be informatized and governed by nm-Gov, where appointments of individuals to official positions within the public apparatus would become a matter of writing data to a database. The conditions, which one would have to fulfill prior to becoming appointed to an official position, would be encoded in the form of CBR locks. These locks would be stored in nm-Gov as any other data, and so could themselves be changed during run time.

As all jural relations would be stored inside the nm-Gov system in the form of informatized entities, advanced use of this data would be made possible with little additional effort. Statistical analyses would become a matter of queries over readily available data, as would requests for access to public information. And as all transactions would be regulated by stored rules, no human moderation would be required. But nm-Gov would not *enforce* transparency—if the sovereign decided to keep decisions from the public in whole or under particular conditions, this would be perfectly doable by defining appropriate CBR locks.

But what about environment policies or law sanctioning sexual predators, drug abusers, embezzlers? Both are not affected by nm-Gov—the latter are to be detected and found guilty by *agents* such as police, prosecutors, and judges, who generate assertions that influence individual legal statuses in the form of jail sentences or penalty payments. Political policies furthermore may coexist with an nm-Gov, as they are nothing more than the expression of *intentions* of groups; they have nothing to do with *data* as it is stored in nm-Gov registries; nm-Gov does nothing to enforce or support them in any way.

Can nm-Gov force tenants to pay their rent? To govern private relations such as the relation between landlords and their tenants, the lease could be considered an obligation for periodic transfer of money. To monitor whether or not their tenants fulfill their obligations, landlords could deploy advanced systems that regularly query the nm-Gov registries to check for received payments. In the case that a tenant would breach the contract, the landlord could use software to automatically take action. Such automated enforcement of jural relations is already today used in the case of subscriptions to software licenses, streaming services, etc.

Does nm-Gov prevent the formation of dynasties? Does it prevent society from falling back into medieval feudalism? It does not. nm-Gov merely provides a technical framework which is agnostic to what happens in the real world.

At the end of the day, nm-Gov provides standardizable access to data, based on which governance can take place. As the model does not imply any limitations on how the data is used, both the private and public sectors of the economy could come up with new ways of how to utilize such data in order to develop new business models, optimized workflows, and so on. The base infrastructure, which would be provided by a real-world instantiation of nm-Gov, has value comparable to that of the networks of roads and railways, the satellite navigation, or the Internet. Properly deployed, the technical layers of nm-Gov would result in a novel dimension of human civilization within cyberspace—a *dimension of digital jural relations*. Chapter 11 will further explore the spill over economic effects of the introduction of new infrastructures.

REFERENCES

de Touzalin, A., Marcus, C., Heljman, F., Cirac, I., Murray, R., Calarco, T., 2016. Quantum Manifesto. European Commission, Brussels.

Duan, L.-M., Lukin, M.D., Cirac, J.I., Zoller, P., 2001. Long-distance quantum communication with atomic ensembles and linear optics. Nature 414, 413–418. https://doi.org/10.1038/35106500.

Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., Li, Y., Shen, Q., Cao, Y., Li, F.-Z., Wang, J.-F., Huang, Y.-M., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N.-L., Koidl, F., Wang, P., Chen, Y.-A., Wang, X.-B., Steindorfer, M., Kirchner, G., Lu, C.-Y., Shu, R., Ursin, R., Scheidl, T., Peng, C.-Z., Wang, J.-Y., Zeilinger, A., Pan, J.-W., 2018. Satellite-relayed intercontinental quantum network. Phys. Rev. Lett. 120, https://doi.org/10.1103/PhysRevLett.120.030501.

Ma, X.-S., Herbst, T., Scheidl, T., Wang, D., Kropatschek, S., Naylor, W., Wittmann, B., Mech, A., Kofler, J., Anisimova, E., Makarov, V., Jennewein, T., Ursin, R., Zeilinger, A., 2012. Quantum teleportation over 143 kilometres using active feed-forward. Nature 489, 269–273. https://doi.org/10.1038/nature11472.

Villoresi, P., Jennewein, T., Tamburini, F., Aspelmeyer, M., Bonato, C., Ursin, R., Pernechele, C., Luceri, V., Bianco, G., Zeilinger, A., Barbieri, C., 2008. Experimental verification of the feasibility of a quantum channel between space and earth. New J. Phys. 10, 033038. https://doi.org/10.1088/1367-2630/10/3/033038.

Yuan, Z.-S., Chen, Y.-A., Zhao, B., Chen, S., Schmiedmayer, J., Pan, J.-W., 2008. Experimental demonstration of a BDCZ quantum repeater node. Nature 454, 1098–1101. https://doi.org/10.1038/nature07241.

This page intentionally left blank

CHAPTER 11

Economic Value of Technological Ecosystems

Contents

In this chapter, we discuss how entrepreneurial ecosystems that evolve around technologies generate economic value and, more specifically, how general-purpose technology (GPT) is a key factor in the emergence of new technological ecosystems. Understanding the economic value of GPT is of high importance in the scope of this treatise, as it provides an understanding of how future investments toward realizing nonmediated governance (nm-Gov) could stimulate the emergence of a new era of prosperity. Hence, investments in research and development toward new GPT that enable nm-Gov are economically justifiable—the economic incentives provided by GPT lead to the development of self-sustaining and self-propagating ecosystems with the potential to exist for eternity.

GPT is a well-known term in economics—the economic value such technologies can generate is seen as an important driver of prosperity. Lipsey et al. (2005) suggested that there are few more than 20 different kinds of known GPT—such as the wheel, steam engine, or the factory system. Per their understanding, a GPT can be classified as a process, a product, or an organization. Lipsey et al.'s definition of GPT has four observable characteristics, namely that it (i) is a single, distinct *generic* technology; (ii) initially has much room for improvement, though it is widely used across the industry; (iii) has many different uses; and (iv) creates many spill over effects.

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00011-X

From an economic perspective, the definition provided by Lipsey et al. is sufficient in order to recognize a GPT after it has been successfully adopted—characteristics (ii) and (iv) will reveal themselves only after a technology has been used for a sufficient period of time. However, the question that this treatise addresses is not how can we recognize a GPT, but rather how can we design one. In order to *design* a GPT, another requirement needs to be taken into account: a GPT must not be designed as a concrete instantiation or product, but rather just as a model. It must be possible for any accordingly capable and skilled person to create concrete instantiations of such a model independently from the author of the original design (Paulin, 2017)—the model, thus, must be an *open model*. The *genericness* of GPTs allows them to be used to either construct infinitely complex systems (as is the case with programming languages) or to be integrated in such. Therefore, the main design characteristics of GPTs are their existence as *open models* and their *genericness*. These design characteristics then enable the rise of ecosystems which gravitate around GPT.

Ecosystems can be defined as self-balancing systems of loosely coupled actors interacting in a shared domain, whereby the interaction is centered around the shared resources (goods, information, services, ideas, etc.) of the ecosystem's domain. Multiple ecosystems can coexist overlapping each other. For example, the forest can be seen as a macro-level ecological ecosystem of animals, plants, microorganisms, etc. Overlapping with the ecosystem of the forest is, for example, the ecosystem of the timber industry or the economic ecosystem of the hunting culture. The latter two both overlap with the monetary ecosystem, the ecosystem of (national/local) politics, and so on.

Technological ecosystems are then those ecosystems which are characterized by the crucial reliance on specific technologies, such as centered around the provision of Web technologies, where the technological ecosystem includes engineers, standards organizations, technology evangelists, and toolset developers devoted to providing resources for Web development. Based on technological ecosystems, advanced ecosystems can emerge, such as the ICT-based online provisioning of tourism services (Gretzel et al., 2015); distributed Internet security (Schmidt, 2014); or other peer-produced infrastructures, tools, and systems (Raymond, 1999). Such ICT-based ecosystems can then be called *digital* ecosystems.

Informatizing governance is essentially about developing new technology to reinvent the way in which governance is conducted. By doing so, existing patterns of governance organization would be disrupted, and it would allow new ecosystems to grow out of the introduced GPTs. In the area of governance, the hope that technology can disruptively transform the way society is governed remains alive among the top scientific challenges, and ideas in this field regularly appear in top scientific outlets.[1]

This chapter provides a closer look at the three types of technological ecosystems, providing a framework for understanding the potentials of technology in creating economic value. Section 11.1 presents the primary ecosystem that evolves directly around a particular base technology and provides the tools and techniques required to further such core technology. Section 11.2 describes the secondary ecosystem, which is about commercializing systems built with the core technology and the tools of the primary ecosystem. Section 11.3 describes the tertiary ecosystem. Tertiary ecosystems evolve on top of platforms built in the course of secondary ecosystems, such as mobile phone apps and plug-ins. Section 11.4 gives an overview of the different approaches to innovation. Section 11.5 provides a concluding discussion, outlining the economic potentials and might of the technological ecosystems.

11.1 THE PRIMARY ECOSYSTEM

GPT comes in the form of nondeterministic models, whereby *nondeterministic* means that the technology does not prescribe which kind of systems will be using it and *model* refers to the descriptive form of the technology, rather than a tangible instantiation. The openness of the models and their technology independence means that anyone can gain knowledge of how to handle them. In turn, this provides economic incentive to teach the technology, to standardize it, to consult on it, or to research toward its improvement and innovation.

The internal combustion engine (e.g., the petrol engine used in cars) is a classic example of a system that qualifies as a GPT. This engine has been invented as a model of a system in which a chamber filled with combustible

[1] One such example is the contribution by Helbing and Pournaras (2015) who stressed the importance of smart technologies, algorithmic governance, and artificial intelligence for governance—though such ideas are perhaps closer to science fiction than to science. What is usually left out in these ideas is the understanding that disruption in the world of technology requires a clear foundation, to trigger progress. Such foundations in the realm of modern ICT are then provided by GPT such as the Internet and the Web technology stacks or artificial languages such as SQL, Java, C, and R.

gas sets a system of hardware components in motion and can be utilized to turn the wheels of a car to drive it. This engine in no way prescribes that it must be utilized for the motion of a car, or that it is any special thing at all that is being moved along a surface of the earth. The combustion engine has been used for turbines, jet engines, electric generators, and a plethora of other applications. Furthermore, the engine design does not prescribe which material is to be combusted—it can be fossil fuels or renewable energy; the engine is nondeterministic in this regard. The separation of the *model* from its *instantiations* (i.e., the tangible systems that are built after the model) allows research and innovation toward better types of engines to take place independently.

The ecosystem which evolves around a newly developed GPT is its *primary* technological ecosystem. The primary ecosystem is the basis for further propagation and evolution of its underlying technology. The primary ecosystem then gives birth to tools (in the case of information technology, these are developer tools such as compilers; debuggers; or integrated development environments like Visual Studio, Eclipse, or MySQL Workbench) and uses optimizations (e.g., the *Gang of Four* object-oriented programming design patterns (Gamma et al., 1995)) and workable instantiations of the models of the technology (e.g., the Apache Web server or the Gecko Web browser engine, which is used in the Firefox browser).

In the case of the internal combustion engine, the primary ecosystem is composed of the research and design activities that cater to the manufacturers of engines, so that these manufacturers are able to produce and improve their engines. It is important to note at this point that the label "primary" for an ecosystem is meant to reflect the relation of the ecosystem to a particular technology and must not be seen as a universal characteristic. In the particular case of the engine, the engine itself is dependent on other technologies, like, for example, appropriate lubricants and coolants, the alloy the engine is molded from, the gas mixture, and ignition systems, each of which can be a core technology on their own, around which their own respective ecosystems develop.

11.2 THE SECONDARY ECOSYSTEM

The propagation of knowledge on and about a core technology provides grounds and incentives for the emergence of a *secondary* technological ecosystem, to utilize the core technology for developing consumer artifacts. In the case of the engine, the secondary ecosystem has picked up the availability of the engine and incorporated it in systems for applied use, such as cars, airplanes, or electric generators used actively as a source of energy to power sound systems at beach parties or to ensure uninterrupted power supply in hospitals.

In the case of the Web, such consumer artifacts are Web pages; Web portals; global mass-consumer systems like Facebook or Amazon; systems enabling business transactions that leverage Web technologies, like the Amadeus CRS[2] for the distribution of travel tickets (cf. Waksberg, 1997), the global credit transfer system for bank transactions SWIFTNet (cf. Zhu, 2002), or academic resource directories like Web of Science or Google Scholar.

The secondary ecosystem comes with self-sustaining economic incentives: it is consumer-/end-user-oriented and, like the primary ecosystem, bears potential for consulting, teaching, standardization, research, innovation, consolidation, integration, etc. The dominating principles of the secondary ecosystem are, however, trade secrets and black-box solutions. Accordingly, artifacts from the secondary ecosystem are closed systems that serve their commercial nature, but their secrecy is in stark contrast to the open and generic nature of core technology.

11.3 THE TERTIARY ECOSYSTEM

Artifacts from the secondary ecosystem can enable the emergence of a tertiary ecosystem by allowing third parties to extend the functionality of the system by means of dedicated interfaces. In the realm of the Web, for example, systems like the Facebook social network or Google's landscape of services and systems provide application programming interfaces (APIs), through which independent developers can develop apps/widgets/plug-ins that are based on the functionality provided by the main systems.

Facebook provides a system of interfaces that allow third-party developers to build their own applications to be hosted by Facebook. This possibility has been used extensively by developers of online games, who have developed mini-games that are seamlessly embedded into the experience of the main Facebook system. Zynga's 2009 FarmVille, a game in which the players manage their virtual farms, is an example of such a system which takes the format of multiplayer online role-playing games (featured in Section 8.2.2). Players engage with the virtual world at no cost, though, in order to advance faster in the gameplay, players are encouraged to make in-app purchases of virtual goods, which they do using real money—thus creating genuine economic value.

[2] *Computer Reservation System.*

Corporations such as Microsoft, Apple, and Google have successfully turned their mobile operating systems into marketplace platforms. Their *Windows Store* (for the Windows operating systems), *App Store/iTunes* (Apple OSX and iOS operating systems), and *Google Play Store* (Android) allow developers to host apps using the operating system's interfaces and sell them to consumers, while paying brokering fees to the market owners. Even though such informatized marketplaces all exist and operate commercially, other systems of interfaces come with no commercial motive, such as the interfaces provided by Web browsers or productivity software like word processors or image manipulation programs. These then provide interfaces which allow "plug-ins" to be embedded into local instances of the systems, by which added value is then generated.

These interfaces then enable the evolution of *tertiary* ecosystems, which rely on the *proprietary* interfaces provided. A developer crafting an iPhone app, developing a Firefox plug-in, or integrating Google maps into its application is thus contributing to the propagation and success of that particular provider's tertiary ecosystem and hence subjects its own system to the terms and conditions of the respective providers. The main characteristic of the tertiary ecosystem is therefore its existential reliance on the technical interfaces, which exist under the sole control of the provider of the main system.

11.4 INNOVATION

One could argue that the role of science is the creation of knowledge (German *Wissenschaft* = the field that creates knowledge). Accordingly, *scientific theories* are encapsulations of verifiable and testable assertions, which as a whole allow the utilization of scientific theory to create predictable, precise, and reproducible results. Disciplines such as architecture, computer science, or informatics cannot use the scientific method to contribute to knowledge. While science creates knowledge in the form of theories, technical disciplines create knowledge in the form of purposeful artifacts. A relevant method used in technical disciplines is thus *design*. Designing is not a theory,[3] and it has no formal structure (Purgathofer, 2006). Instead, designing is about creating or improving artifacts that provide solutions for specific

[3] Bannister and Connolly (2015) briefly mention *design theory* without closer examination of the issue. It is true that *design theory* is an existing field of study that attempts to find recipes to support/structure design, but as Purgathofer (2006) emphasizes, even early influential scholars in design theory, such as Christopher Alexander, soon retracted their support for the relevance of this field ("I would say forget it, forget the whole thing").

problems, or about designing radically new contributions to human knowledge in the form of abstract concepts, models, or concrete instantiations. The creation of something new is then called *innovation*.

Drawing from the vast literature on design, Hevner et al. (2004) describe the role of design in the area of software engineering and information systems research. They divide research methods used by technical disciplines into two paradigms: *design science*, concerning the creation of artifacts, and *behavior science*, to deal with the evaluation of such artifacts in real environments. Design artifacts "are broadly defined as *constructs* (vocabulary and symbols), *models* (abstractions and representations), *methods* (algorithms and practices), and *instantiations* (implemented and prototype systems)" (Hevner et al., 2004).

When innovating design science artifacts, one must keep in mind that only innovations in design that are of significant relevance can be deemed as a contribution to human knowledge:

> *One issue that must be addressed in design-science research is differentiating routine design or system building from design research. [. . .] Routine design is the application of existing knowledge to organizational problems, such as constructing a financial or marketing information system using best practice artefacts existing in the knowledge base. On the other hand, design-science research addresses important unsolved problems in unique or innovative ways or solved problems in more effective or efficient ways. The key differentiator between routine design and design research is the clear identification of a contribution to the archival knowledge base of foundations and methodologies.*
>
> ***(Hevner et al., 2004)***

An awareness for the distinction between design innovation and construction based on established practices is crucial in disciplines such as software engineering (which also affects e-Gov), where innovative new systems (or new usages of systems) often stem from functionally combining already existing systems into more complex system-of-systems.

Innovation itself comes in two flavors—it can be either incremental or radical (Binks, 2014). In the context of design, incremental innovation is the improvement/alteration of existing design, while radical innovation is the invention of something (radically) novel, which did not previously exist. "Add successively as many mail coaches as you please," wrote Joseph Schumpeter in his *The Theory of Economic Development* (cf. Binks, 2014, p. 92), "you will never get a railway thereby." "Breeding home pigeons that could cover a given space with ever-increasing rapidity did not give us the laws of telegraphy, nor did breeding faster horses bring us the steam locomotive" wrote Edward Menge (Binks, 2014) to likewise emphasize the importance of radical innovation.

Whether an invention is to be considered incremental or radical innovation is often a matter of perspective: For example, most contemporary kitchen stoves are either gas stoves or glass-ceramic stoves (which superseded stoves that used iron hotplates). A radical novelty which enabled rapid evolution of the modern Western kitchen stove was Benjamin Thompson's *Rumfold fireplace*. This late-18th-century sensation brought smoke-free cooking (though still on an open fire) as a novelty to Britain. Fueled by the success of his fireplace, which remains a characteristic feature of many British homes to this day, Thompson invented a brick stove with holes at the top, such that pots could be securely positioned for cooking. In the 19th century further radical innovation followed in the form of cast iron stoves in which fire heated iron plates that were mounted on top of the oven. This in turn defined the appearance and functionality of the modern stove and allowed for the fusion of the kitchen and the dining room. From this point on, if seen from the perspective of the stove as a functional element of the modern apartment, the next innovations in the evolution of the stove were incremental: the electrical stove exchanged the fire for electricity and, after that, the iron plates were changed for glass-ceramic plates. If we zoom in closer and focus on the evolution of the stove top, further milestones can be deemed radical innovations: cast iron as a new technology applied to the stove, then gas replaces wood/coal, then electricity replaces fire, then glass-ceramic replaces cast iron, etc.

Both incremental as well as radical innovation can contribute knowledge, which is sufficient to deem such contributions as relevant in the scope of design science. Patents and doctoral theses from computer science or informatics will typically come in the form of technological inventions of either type.

Radical innovation bears potential for *transforming* industry, economy, and society. The invention of the combustion engine has reduced animal-based transport to the level of tourism and sport, just as the successful application of the screw propeller to ships has transformed naval transport and reduced sailing to a mere leisure activity; the introduction of electricity-based household appliances (kitchen stove, washing machine, dishwasher) has transformed society by making time available for leisure and eliminating the need for household servants; etc. Incremental innovation on the other hand is crucial for the ripening process of technology, as well as its further development and fortification—it is due to incremental innovation of the underlying technology that early flying machines have been transformed into the safe commercial aircrafts of today.

11.4.1 Innovating for Governance

The history of political order (Fukuyama, 2012; Graeber, 2015) is a story of design science applied to human society. Technological and organizational innovation—new important types of raw material (copper, iron, petroleum), new weaponry knowledge (bow and arrow, guns, guided missiles), new means of communication (post system, telegraphy, wireless transmission, the Internet), new means of transport (ships, airplanes, trains), etc.—go hand in hand with the rise and fall of empires and civilizations, of trade routes and monopolies, of organizations, of ideologies, of religions, and of the manifold possibilities to erect and maintain systems of political order. The parliament, the rule of law, democratic legitimization of authority, public schools, and public health care, etc., are nothing but radical innovations that were thought up at some point in time and introduced to society by new stakeholders of power, who praised them as the building blocks beneficial to progressive order.

Inventions of new technologies and their advances give opportunities to apply them for the invention of new paradigms in other domains. Even the technological evolution of the kitchen stove, driven by Benjamin Thompson's discovery of the clean-burning stove, was an important enabler of urbanization, as smoke-free cooking eliminated the need for dedicated kitchen rooms (the *Rauchküche/Schwarzküche* or "black kitchen," as it was called in German due to the soot coloring the room black), and allowed the transformation of the kitchen into a compact living room. Further advances in technology significantly reduced the skill and time required to prepare meals, as well as other household chores, resulting in the opportunity to rethink and politicize the traditional role of *the housewife*, formerly an essential asset to households that could not afford servants.

The history of the kitchen stove demonstrates how technology can open new opportunities for change in society and political order. Electric household appliances, such as the electric stove, the washing machine, and the dishwasher, gave the working man opportunity to run a household independently, making the societal institution of *the housewife* obsolete—the roles and functions of man and woman in cohabitation could be rethought. Just as technology changed the household by making old patterns of conduct obsolete, it changed patterns of manufacturing and other domains. Radical technology, which matured throughout the 20th century (electronics, computing technology, communication technology, and information technology) enabled computerization and informatization (see Chapter 7), allowing established methods and practices in manufacturing (Zuboff, 1988), as well as political and societal institutions, to be challenged.

The 20th-century housewife's question of "Why should I stand in the kitchen—*he* could cook for himself" bears a certain resemblance to the present-day schoolchild's question of "Why do I have to go to school—I could read it all up on the Internet." Another such line of questioning of established institutions was instigated by the rising middle class in Europe in the 19th century, who asked "Why should the royal court decide how taxes are spent?" This question led to the creation of the modern parliaments and modern popular politics. Similarly, modern parliaments are faced with the question "Why should the parliamentarians decide how taxes are spent?" Due to the evolution of modern informatics this question can be further addressed, and new approaches to collective decision-making on such matters can be thought up.

Technological inventions and innovations create the opportunity for new ideas to emerge. The newly thought-up concepts are first developed into theoretical models and are validated by means of thought experiments. If feasible, the ideas are explored in laboratory environments, such as living labs, and finally tested out in the wild. The design of new concepts and ideas follows the principle of the design cycle (Wieringa, 2009), whereby feedback from real-world application is fed back into the next iteration of the design cycle, until maturity is reached.

11.5 DISCUSSION: THE ECONOMIC OPPORTUNITY OF INNOVATION FOR GOVERNANCE

The way in which the public perceives technological progress is determined by the outputs of the secondary ecosystem. Such outputs could be airplanes, smart phones, Web sites, etc. The outputs of the secondary ecosystem are also the basis for technology-focused deliberations in politics and marketing, or technology-focused studies in social sciences, such as the social construction theory (cf. Hofkirchner, 2007) which aims to explain how technology and society affect each other.

Accordingly, if a powerful corporation launches a new consumer product on the market, such as a new version of their smart phone, the features of this new product (e.g., new camera technology, new communication capacities) will be advertised through strong marketing campaigns aimed to stimulate the consumption of their product. Likewise, if this corporation wants to kick-start a tertiary ecosystem by providing, for example, an online marketplace for the distribution of their apps, this market place will be hyped and praised through the media as something exciting and trendy.

However, all the products born by the secondary ecosystem would not exist without the primary technological ecosystems and their propagation. Unlike the secondary technological ecosystems, which are pushed by the mighty machinery of international corporations, the invention of core technology and the development of primary ecosystems are often driven by voluntarism of individual enthusiasts. Raymond's (1999) *The Cathedral and the Bazaar* provides an account of how independent software developers from all around the world coproduce valuable open-source software in their spare time, out of mere enthusiasm. An example of such a software born out of voluntarism is Linux, which serves as the backbone of the widely used mobile operating system Android.

Each of the three technological ecosystems has the potential to sustain and perpetuate itself as long as possible. Among the factors that keep the ecosystems alive are the individual's motivation to create independently and make a mark (which is crucial in primary ecosystems where funding is scarce), commercial interest, and the self-preserving urge of organizations.

11.5.1 The Public Apparatus: A Very Different Animal

The focus of modern ICT's primary ecosystems was on delivering advanced digital *communication* of data or information, to be used for computerization (digital computer-enabled automated processing), virtualization (emulation of resources), or informatization (control of real-world technical or nontechnical systems by means of ICT). Such technization of communication has enabled the rise of technical ecosystems and their adjacent economies, and facilitated the rise of global players such as Google and Facebook. This was possible for the simple reason that the technization of *communication* was sufficient to build the complex systems such as those required by Facebook, since any Web site (from a technical perspective, Facebook is no more than a Web site) at its core is about the *communication* of data between the Web server and the Web client (if seen from a technological perspective), or between the organization and its customers.

Governance of the public apparatus goes beyond mere communication: it is about collective decision-making; about the control of resources, power, and social services; and about systems of law and belief, such as the fiat monetary system or fiat social security system. Needless to say, all of these aspects include communication, but they also introduce constraints and requirements which exceed the scope of the capabilities of the present-day ICT landscape. Compared to communication and trade, *governance* is a wholly different kind of beast: while the functionality of Facebook can be provided to its *markets* of prosumers, advertisers, or intelligence agents as is, a public apparatus cannot (or rather must not) be subjected to systems with locked functionality, but instead must be able to flexibly extend/contract/limit/release the functionality and constraints of its systems of governance to its fullest extent.

The otherness of societal governance as compared to market-oriented products is a reason why established approaches from e-business do not and cannot work in e-Gov (discussed in Chapter 2). On the other hand, this otherness bears great potential to develop new primary ecosystems, which could sustainably open societal governance to the might of technical research and development.

11.5.2 Might of Technical Ecosystems: A Win-Win Situation

The power of global players of the dot-com era, such as eBay, Uber, Airbnb, Alibaba, Facebook, Twitter, Google, Apple, or Tencent, is owed to the possibilities of the secondary ecosystem. The products of these companies are themselves a part of the secondary ecosystem, which they have helped to raise to prominence and economic might. With the creation of tertiary ecosystems enabled through APIs, these companies have significantly expanded their outreach and increased their revenues by harvesting the fruits of their digital orchards. Meanwhile, the economic might of technological ecosystems has reached an impressive scale: California's economy—substantially due to the power of the Silicon Valley—is said to be the eighth largest economy in the world, outperforming the economies of Russia or Italy (ccsce.com, 2015). The existence of these global players is not possible without the underlying existence and perpetuation of the primary ecosystem.

The knowledge and energy beyond that which can be utilized in the primary ecosystem fuels the secondary and tertiary ecosystems. For example, students, academic researchers, and enthusiasts, who in their spare time contribute to the development of tools and systems that make up the primary ecosystem, can become valued employees and innovators of the industries that make up the secondary ecosystem. Accordingly, the surplus knowledge and innovative spirit from the primary ecosystem pioneer the commercial innovations in the secondary and tertiary ecosystems, and keep perpetuating their evolution.

The value of openness and nondeterministic *genericness* of core technology for democratic action and *anarchic* (as in *without government*) production has proved itself duly during the Browser Wars (Gromov, 2011), where the once one-and-only Netscape Web browser was first superseded by Microsoft's Internet Explorer, which in turn was ousted by the open-source-first (though Netscape-sponsored) competitor Mozilla (Firefox). The success of Linux, itself an open-source-first project, is yet another—and even the most prominent one—confirmation of democratic potentials to rival economically motivated solutions.

Another typical GPT in ICT is the core WWW stack, which comprises the HTTP protocol for making requests on the Web, the HTML mark up language which describes how Web pages look, the CSS presentation system for visually designing Web pages, and the JavaScript programming language.[4] The openness and the existence in the form of models of these core artifacts allow anybody to build their own Web server, Web browser, Web page, or Web search engine from scratch and do so independent of the tools and technology used to realize the instantiations.

The ability to gain knowledge about and on GPT implies potential to hinder monopolization and feudalization of derived ecosystems: by knowledge of the particular GPT, anybody can build a new and better social network system, a new and better operating system, or a new and better Web browser, much like anybody can write a book or verify a mathematical equation, because the underlying knowledge required—i.e., knowledge of the alphabet or the algebraic system—comes as *open* and *generic* artifacts.

The openness and genericness of GPT thus prevent phenomena such as vendor-lock-in situations or the monopolization of knowledge. From the perspective of future democracy, this is a win-win situation. The openness and neutrality of GPT manifest democratic and liberating potentials, while the technological ecosystems enabled by new GPT create new work and new jobs and stimulate the economy.

[4] Adjacent Web-related base technologies such as XML, DOM, and HTML5 can be added to this list without harming the argument. Proprietary Web-related technologies such as Flash, on the other hand, do not fit the definition of base technology.

REFERENCES

Bannister, F., Connolly, R., 2015. The great theory hunt: does e-government really have a problem? Gov. Inf. Q. 32, 1–11. https://doi.org/10.1016/j.giq.2014.10.003.

Binks, M., 2014. The crucial role of universities in promoting radical innovation. In: Greenaway, D., Rudd, C.D. (Eds.), The Business Growth Benefits of Higher Education. Palgrave Macmillan UK, London, pp. 91–108.

ccsce.com, 2015. California Remains the World's 8th Largest Economy.

Fukuyama, F., 2012. The Origins of Political Order: From Prehuman Times to the French Revolution, Paperback ed. Profile Books, London.

Gamma, E., Helm, R., Johnson, R., Vlissides, J., 1995. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley Professional Computing Series. Addison-Wesley, Reading, MA.

Graeber, D., 2015. The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy. Melville House, Brooklyn/London.

Gretzel, U., Werthner, H., Koo, C., Lamsfus, C., 2015. Conceptual foundations for understanding smart tourism ecosystems. Comput. Hum. Behav. 50, 558–563. https://doi.org/10.1016/j.chb.2015.03.043.

Gromov, G., 2011. The Roads and Crossroads of Internet History—Chapter 4: Birth of the World Wide Web [WWW Document]. http://www.netvalley.com/intvalweb.html. (Accessed 23 December 2015).

Helbing, D., Pournaras, E., 2015. Society: build digital democracy. Nature 527, 33–34. https://doi.org/10.1038/527033a.

Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design science in information systems research. Manag. Inf. Syst. Q. 28, 6.

Hofkirchner, W., 2007. A critical social systems view of the internet. Philos. Soc. Sci. 37, 471–500. https://doi.org/10.1177/0048393107307664.

Lipsey, R.G., Carlaw, K., Bekar, C., 2005. Economic Transformations: General Purpose Technologies and Long-Term Economic Growth. Oxford University Press, Oxford, New York.

Paulin, A., 2017. E-Gov theory and the role of design science in transforming public governance. Presented at the 18th International Conference on Digital Government Research, New York. https://doi.org/10.1145/3085228.3085300.

Purgathofer, P., 2006. Is informatics a design discipline? Poiesis Prax. 4, 303–314. https://doi.org/10.1007/s10202-006-0029-0.

Raymond, E.S., 1999. The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary. O'Reilly Media.

Schmidt, A., 2014. Secrecy versus openness: Internet security and the limits of open source and peer production (PhD thesis). TU Delft, Delft, Netherlands.

Waksberg, R., 1997. The Future of Global Distribution Systems: The World Wide Web as an Alternative Travel Distribution Channel (MSc thesis). University of Surrey, Surrey, UK.

Wieringa, R., 2009. Design science as nested problem solving. Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology. DESRIST'09. ACM, New York, NY, USA, pp. 8:1–8:12. https://doi.org/10.1145/1555619.1555630.

Zhu, D., 2002. Security control in inter-bank fund transfer. JECR 3, 15–22.

Zuboff, S., 1988. In the Age of the Smart Machine: The Future of Work and Power. Basic Books, New York.

PART IV

Code as Law

This treatise so far has focused on defining a conceptual model for non-mediated governance (nm-Gov): Part I defined the context and provided a critique of contemporary approaches to modernizing governance by means of technology. Part II provided an understanding of the "nuts and bolts" of systems of law, which has traditionally empowered the agents of governance. Part III explored how technology can be used to control structure and elaborated on a model for nm-Gov that could supersede established models for governance. This part deals with technical details and the knowledge required to appropriately design the required technical infrastructure. This infrastructure should make it possible to store and retrieve jurally relevant data without human moderation. At the same time, this infrastructure should make it possible to govern requests for the access to data by rules, whereby the semantics and structure of neither the requests nor the rules could be predictably known at the time of design. Aside from this, concrete approaches to satisfy the functional and technical requirements that impact the architectural aspects of the solution (as defined in Chapter 10) will be discussed.

This part is composed of three chapters, each of which aims to address a particular relevant aspect in the search for appropriate technology. Focus is laid on the possibilities provided by tools and techniques that are readily available at the moment or are subject to research. To this end, Chapter 12 aims to outline various readily available technologies and discuss their limits in regard to their applicability for nm-Gov. Chapter 13 describes a general-purpose technological system for describing the rules for governance (law in the form of code) that can then serve as a basis for informatized governance or other areas of application. Chapter 14 discusses four different scenarios that aim to illustrate the application of nm-Gov to examples taken from the real world; with this, this chapter aims to explore possibilities for transformations in the respective scenarios.

The esteemed reader is warned up front that the contents of this part are highly technical and hence require a deep level of insight into the world of ICT. Readers who do not feel comfortable with the deliberations on technological details may safely skip the first two chapters to Chapter 14, which brings forward reasons for the feasibility and superiority of informatized governance.

CHAPTER 12

Choosing Fitting Technology

Contents

The nonmediated governance (nm-Gov) electronic registries impose six functional requirements (Section 10.2) that affect the choice of usable technologies. The system of electronic registries (1) must consist of nodes whose location in the network can be defined through law such that everybody is able to know where to reach them, (2) must provide a clear message exchange protocol such that everybody is able to know how to communicate with it, (3) must provide a transparent and legally definable processing logic such that everybody is able to know how their request will be processed, (4) must not restrict queries for data in their content such that every imaginable request can be made, (5) must ensure *fair nonrepudiable* communication such that a requester can rest assured that their request was received, and (6) must not restrict access to the stored data beyond the legally imposed restrictions.

The objective of this chapter is to identify the existing technologies which could be utilized to satisfy these functional requirements. The selection of technology analyzed is not intended to be normative, but rather to be understood as a feasible selection derived from an informed opinion. The discussion of the selected and analyzed technology is an entry point into a broader professional deliberation to help form a thorough knowledge base for determining which technology can be used for nm-Gov.

Section 12.1 first investigates the possibilities for storing and retrieving data in the context of the nm-Gov registries, in accordance with requirement 4. Sections 12.2 and 12.3 address requirement 5 with regard to

https://doi.org/10.1016/B978-0-12-816224-8.00012-1

fair nonrepudiable message exchange (Section 12.3) and electronic identity (Section 12.2).

The other requirements do not pose essential research challenges and, hence, are not discussed here: Requirement 1 is trivial to realize—it only takes the implementation of some central registry containing the addresses of the individual nm-Gov electronic registries in use (in case there are many) and an agreement (e.g., a constitution) that defines where this central registry is located. Requirements 2 and 3 are a matter of professional choice and open-source style of engineering, which again do not constitute a research challenge that requires broader deliberation.[1] Requirement 6 will be discussed in Chapter 13 in further detail.

12.1 STORING DATA, QUERYING DATA, CONTROLLING ACCESS TO DATA

In order to comply with the functional requirements, nm-Gov registries must store data in such a way that it can be read and written in an analogue manner, meaning that an appropriate artificial language must be available through which various operations on the stored data can be expressed. Further, electronic registries must provide access to the *core* data, implying that the data structures must be transparent to the user.

In the section on open government data (Section 2.1.4), the question "at which point can data be considered *core data*" was raised. While we will not be attempting to answer this question here, we elaborate on the definition of "core data." Let's start with the case of a land registry to illustrate the granularity required for data to qualify as *core* data. To this end, let us assume that *Ann* owns land in Vienna, and so a typical data entry denoting her ownership of land parcel no. *1084/8* of the Viennese sixth district (post code 1060) might be stored as shown in Table 12.1.

The granularity of this example is sufficient, as the stored data clearly identifies the subject/items at stake. The identifications used here may be references

Table 12.1 Sample land registry data

```
{
  subject_id:       Ann,
  legal_relation:   ownership,
  land_parcel_id:   1060/1084/8
}
```

[1]A prototype instantiation of the nm-Gov registry is documented in Paulin (2015).

to broader concepts; for example, the field `subject_id` is a reference to further data about the subject stored elsewhere; `land_parcel_id` could be a reference to a concept that would describe a geometrical piece of land through GPS or a similar system. The data stored in the field `legal_relation` in this case stores core data in its finite, semantic form, and bears meaning for whomever requires its use, e.g., use by a law enforcement agent to protect ownership.

Core data can thus appear in either its semantic *final* form or as a *reference* to other concepts. The *reference* form is not a separate entry type, but rather a foreign key for which other registries (either physical or logical) could store more linked data—a subject identifier, for example, could be used by a large number of separate nm-Gov registries, as in the case of the Danish Central Citizen Registry described in Section 2.1.1.

For describing *constellation-based eligibility evaluation* in Section 9.2, set theory and relational algebra were used. Accordingly, it would seem logical to utilize relational databases, as they are the predominantly used data storing structures in the information systems of today. Though the nm-Gov model does not define the internal structure of the stored data or how it is organized in the electronic registries, one reasonable option would be to utilize the existing relational database management systems (RDBMSs), as they generally implement the standardized query language (SQL), derived from relational algebra and calculus (Codd, 1970).

SQL is an artificial language which is used to interact with data. The language encompasses commands that are used to read or write data and to perform complex queries in order to retrieve the stored data. SQL can be used to collate datasets, filter data by its characteristics, etc., without limits to the complexity of the composed queries. Furthermore, as the relational data model does not define how exactly the data must be stored physically within the database system, SQL remains platform- and vendor-independent.

12.1.1 Fine-Grained Access Control

SQL, however, does not provide explicit mechanisms for the regulation of access privileges for the data itself. Hence, vendors of RDBMSs implement their own solutions, whereby access can often be restricted on the level of schemas (databases) and relations (tables). Means to govern access on the level of tuples (rows of a table) have only been marginally implemented in commercial products by, e.g., Oracle and Sybase.

> *In Oracle's Virtual Private Database (VPD) authorization mechanism, each relation has a set of access control functions that are specified by the administrator.*

> *Separate functions can be specified for different types of access (e.g., SELECT, INSERT, DELETE). The functions take as argument elements from the secure query context, and return predicates which are logically 'AND'-ed with the WHERE condition of the SQL query. In the case of data items for which access is not allowed, VPD may eliminate tuples from the result set altogether, or replace unauthorized cells with special NULL values. Similarly, Sybase allows different predicates to be specified for each table column, and the predicates are appended to the WHERE condition of the queries at execution time.*
>
> ***(Bertino et al., 2011, p. 69)***

Bertino et al. (2011) distinguish three types of *fine-grained access control* mechanisms in relational databases: query rewriting, SQL extensions, and transparent authorization views (common predefined result sets of stored queries). For the query rewriting approach, Bertino et al. provide the example of LeFevre et al. (2004) who enquired into the requirements of Hippocratic databases—i.e., databases which store sensitive medical data about patients. Their approach was to allow each owner of a tuple (i.e., the patient) to decide which data was allowed to be revealed for a given purpose, whereby the purpose is defined via categories—a category for billing purposes and another for medical research use, for example. In this case, the access authorization data was stored as separate metadata, and access to each tuple was governed by an entry in the corresponding metadata relation. This approach applies hard-coded categories to cater to the question "for which purpose is data accessed," as well as identity-based regulations to restrict access based on the recipient of the requested data. "At runtime, the [database management system] extracts the necessary information from the secure context and rewrites the query in accordance to the permissions mandated by the data owners" (Bertino et al., 2011, p. 72).

Chaudhuri et al. (2007) suggested to extend the SQL specification in order to make fine-grained access control possible. Their main idea is "to extend the existing access control grant mechanisms to handle conditions that are expressed as a function of the query execution context. Such clauses are called *predicated grants*. The predicates are specified in a parametric fashion when the policies are created, and are evaluated at runtime to decide which set of tuples in the result set will be returned to the user. The actual technique of enforcement is similar to query rewriting, but the SQL language extension is specified at a declarative level, therefore no restrictions are placed on the mechanisms used to implement predicated grants" (Bertino et al., 2011, p. 77).

Alas, neither technique caters to the requirements for fine-grained data access in nm-Gov electronic registries—we shall discuss this in Section 13.1.

In business applications, it is common for system developers to resort to hard-coding authorization procedures into the program logic of the software in such a way that a change in the authorization mechanism would require an update to the software. However, such an approach does not provide the temporal sustainability that is required for nm-Gov and constrains systems to depend on *god-like* developers and administrators.

12.1.2 Resource Description Framework (RDF)

The RDF plays an important role in the Linked/Open Data movements and the Semantic Web, as discussed in Section 8.1. The RDF is a syntax-neutral framework for storing data in "subject-predicate-object" triples, whereby the subject denotes the described resources, the predicate its attribute, and the object its value. Various syntaxes for expressing and communicating RDF exist, such as RDF+XML, N3 (Berners-Lee et al., 2008), or Turtle (Beckett and Berners-Lee, 2008).

The inventor of the Web, Tim Berners-Lee, views RDF as an essential technology for the online publishing of data in a way that allows intelligent reuse and integration of remote sources of data. Publishing data linked through RDF would result in the *Semantic Web*, an interlinked network of knowledge for advanced systems to use (Berners-Lee, 2009). However, RDF was designed to contain structure and not semantics—semantics were only introduced around 2004 (Patel-Schneider, 2010). Furthermore, the semantics aspects of RDF are not relevant for nm-Gov, as the meaning of data stored in the electronic registries is to be defined and determined by the context (e.g., law). Thus, there is no need for any kind of metadata that would store semantics as implied, e.g., by the Semantic Web vision.

The RDF is a model that is based on the graph theory (Berners-Lee, 1998; Hayes and Gutierrez, 2004) and is in sharp contrast to the relational model for storing and querying data. Although RDF was not designed as a database technology, but merely as a model for representing data, an option might be to consider the use of triple-stores, i.e., dedicated graph databases for storing RDF. Graph databases are among the oldest database concepts, though they only gained popularity recently due to the choice of global enterprises like Google, Facebook, LinkedIn, or Amazon, who use them in situations where they need to process large quantities of data efficiently for better performance (Vicknair et al., 2010).

In comparison to relational databases, graph databases lack a common query language. Angles and Gutierrez (2008) list a wide assortment of languages used to retrieve data from graph databases: G+, GraphLog, Gram, PaMal, GraphDB, and Lorel, as well as languages dedicated for querying RDF, namely RQL, SquishQL, RDQL, RDFQL, TRIPLE, Versa, SeRQL, and RXPath. In 2004, the SPARQL query language for RDF appeared, a W3C recommendation since 2008. Although originally a language only for read querying data, SPARQL later received the amendment SPARQL-Update, which enabled write access to RDF data (Seaborne et al., 2008). A range of access control mechanisms for SPARQL endpoints are available, such as W3C's decentralized *WebAccessControl* system[2] or various other approaches in early research stages (cf. Costabello et al., 2012).

Both SQL and SPARQL offer similar functionality with regard to allowing read/write access to data that can be governed by appropriate access control mechanisms. In principle, both might be considered for use in nm-Gov registries. While SQL has been established as a technology for several decades, SPARQL was designed with the distributed architecture of the Web in mind. Although both options seem feasible at first glance, the choice for this treatise is to focus on using relational databases and the SQL language, for the reason that it is a mature, standardized technology with undisputed market dominance.

12.2 IDENTIFICATION, AUTHORIZATION, AND DATA INTEGRITY

The functional requirement 5 (fair nonrepudiable communication) implies that any transmitted message must be ensured full integrity, while the authorization control mechanism of the electronic registries implies that the identity of the requester must be transmitted together with the message in a nonrepudiable manner.

There are a number of readily available technologies that can be used for identification and authorization. Various single-sign-on (SSO) technologies allow users to identify themselves to heterogeneous servers using a single identity. David et al. (2011) identify Kerberos, OpenID, and Snap2Pass as relevant SSO options. Kerberos (Miller et al., 1987) was one of the first SSO protocols for authorizing access to remote services in a network. Its core architecture uses two tightly synchronized servers, the authentication server that verifies the identity of the client and a ticket server, which issues time-limited tokens (tickets) for accessing services. David et al. note that the protocol is not only highly complex, but from today's perspective is also no longer adequately secure.

[2]http://www.w3.org/wiki/WebAccessControl.

OpenID (Recordon and Reed, 2006) is an open standard for SSO over the Web. It does not depend on a central authority to issue identities; consequently, users can choose from various identity providers. The individual authentication to identity providers can require the user to enter a basic username/password combination, but advanced biometric and smartcard authentication are also possible. After authenticating the user, the server issues a Yadis-document (Miller, 2006), which is then used for identification to applications. OpenID is significant because of its popularity—it is used by Google, Yahoo, MySpace, AOL, PayPal, VeriSign, etc. However, OpenID is neither designed to provide message integrity nor the nonrepudiation of its content, thus it would not meet the requirement 5 of the nm-Gov electronic registries.

Snap2Pass (Dodson et al., 2010), likewise, would not be suitable for nm-Gov for the same reason. Snap2Pass is a protocol that authenticates the user by presenting them with a randomly generated *QR code*.[3] The user must use their mobile phone, on which a shared secret is stored, to capture the QR code. Using that shared secret and the unique token received by capturing the QR code, a hash-based message authentication code (HMAC) is generated and returned to the server.

A survey by Akram and Hoffmann (2008) also considered the aspect of nonrepudiation when evaluating six popular technologies—SAML, OpenID, CardSpace, Shiboleth, Higgins, and Liberty. They found that only Higgins, a kind of distributed open-source social network where personal data can be hosted on one's own server,[4] was capable of adequately providing nonrepudiation. Higgins was also the best recommendation for user-centric identity management in a survey conducted by El Maliki and Seigneur (2007).

The broad assortment of available and constantly evolving technologies for identity management suggests that choosing a conservative, well-established technology makes more sense in the context of designing further complex systems. From this perspective, the well-established X.509 ITU standards for the *public key infrastructure* (PKI) provide a sound option for management of identity.

The X.509 standards describe an architecture that provides the concept of *digital certificates* issued by identity providers, who act as *trusted third parties* (TTPs). A digital certificate is an electronic token that identifies a subject

[3]Quick response codes are two-dimensional barcodes—machine-readable optical labels containing information.

[4]http://www.eclipse.com/higgins.

and has been signed by the TTP by means of the electronic signature. The electronic signature can be achieved through asymmetric cryptography which involves two mathematically linked *keys*, one of which—the private key—is known only to the signer of a message. Applying the public key to a message signature proves that the signature could have been created only with the private key, which is assumed to be known only to the signer. By digitally signing a message, we can thus achieve its integrity during communication (tampering with the message would render its signature invalid), nonrepudiation of origin (the author of a message cannot plausibly deny having created it), and identification.

At first glance, the X.509 digital certificates provide a clear solution for identification. However, the devil is in the details, that is, when it comes to choosing the appropriate cryptographic technologies for concrete cases. This is because X.509 merely defines the structure of the digital certificate, not the cryptographic algorithms that are used for signing. In practice, this requires it to agree on which concrete algorithms to implement in the systems of the participating parties.

In Section 4.1.2, the case of the Austrian *Citizen Card* was discussed, demonstrating what can go wrong if X.509 is deployed with exotic cryptographic algorithms. There, two carrying technologies have been developed to convey the digital certificate, namely a smartcard and a mobile solution. In the case of the mobile solution, the certificate is stored in a hardware security module on a high security server, access to which is granted through a multifactor authorization involving one's mobile phone. Both options chose an *elliptic curve cryptography* (ECC) approach to deliver signatures using the *elliptic curve digital signature algorithm* (ECDSA),[5] whereby the concrete ECC *curve* chosen was the P-192, as standardized by the *National Institute of Standards and Technology* (Bauer, 2009). The P-192, however, is not well accepted by popular and enterprise-level software, which mainly supports the set of algorithms listed in the US *National Security Agency's* (NSA's) *Suite B*.[6] For example, Suite B algorithms have been implemented in the Microsoft Windows operating system since Windows Vista, where they are available to applications and higher-level programming frameworks such

[5]ECDSA is one of a few widely known algorithms for calculating digital signatures. Other such algorithms are the RSA and DSA algorithms.

[6]Suite B contains nonclassified government-level algorithms which are to be used by US government agencies for transmitting sensitive and classified information. A "Suite A" also exists, which contains classified algorithms for tasks where the highest confidentiality is required.

as Microsoft .Net (Bauer, 2009). Alas, P-192 is not part of Suite B and due to its marginal popularity third-party analysis of signatures generated by existing implementations of the Austrian Citizen Card becomes virtually impossible (Klemen, 2012).

When considering which technology to use for conveying identity in nm-Gov, special care must be taken to find a sustainable solution. X.509 is a sound option for storing identity; however, it involves a strict hierarchy of cascading identity providers (each higher identity provider vouches for the integrity of the lower). In the context of nm-Gov, this hierarchy could potentially be beneficial, as identity within nm-Gov electronic registries can be a local matter rather than a global one, meaning that theoretically a subject could have multiple domain-specific identities. As an alternative to the certificate-based PKI, one might consider identity-based PKI in which the originator's public key is not conveyed through a digital certificate but rather derived from the originator's identifier (Hölbl, 2009, p. 22). Anyhow, sustainable identity management for nm-Gov is a topic which requires deeper research.

12.3 NONREPUDIATION IN MESSAGE EXCHANGE

It is essential in nm-Gov that each message transaction is fully nonrepudiable. This means that both the sender and the receiver of a message must be sure that the transaction between the parties occurs as intended, as this is the only interaction that takes place. If the requesting party is not able to be sure, with reasonable certainty, that the request was received, this would jeopardize the integrity and suitability of the system of electronic registries.

In the real world, this kind of message delivery would be handled through certified mail delivery—we are accustomed to transmitting letters, documents, and other items to the addressee using certified mail, which gives a valid proof (even before court) that the item was dispatched, handled, and ultimately received by the addressee. In the real world, the person addressed must confirm the receipt of the item with their signature—this process of delivering the item and returning a proof-of-receipt is handled by the postal service provider, a TTP, trusted by both the sender and the receiver of the message. The TTP thereby assures that neither party can repudiate having participated in the exchange. This type of exchange is called *fair nonrepudiation* (FNR).

In cyberspace, FNR is provided by *certified e-mail services* (CeMSs), whose aim is to provide an assortment of nonrepudiable evidences; the following definitions of nonrepudiable evidences are generally accepted (Ferrer-Gomilla et al., 2010; Tauber, 2011):

- *Nonrepudiation of origin* (NRO): A protocol provides NRO if, and only if, it generates evidence of origin, which allows the *recipient* to demonstrate to an arbiter whether or not the originator was the message's author. Such evidence can be generated, e.g., by means of a digital signature.
- *Nonrepudiation of receipt* (NRR): A protocol provides NRR if, and only if, it generates evidence of receipt, which allows the *originator* to demonstrate to an arbiter whether the recipient received the message.
- *Nonrepudiation of submission* (NRS): A protocol provides NRS if, and only if, it gives evidence against the false denial of having submitted the message. (This evidence is generated by the sender's message transfer agent[7] and is addressed to the sender.)
- *Nonrepudiation of delivery* (NRD): A protocol provides NRD if, and only if, it provides evidence against the false denial of having delivered the message. (This evidence is usually generated by the recipient's message transfer agent and is addressed to the sender.)

Ferrer-Gomilla et al. (2010) emphasize that there is no clear understanding of which evidence must be part of the exchange. Thus, they first suggest an initial definition that a CeMS can be defined as the exchange of a message plus NRO for NRR, but show that this definition would be rejected by others (Zhou and Gollman, 1996), who do not consider NRO evidence mandatory. Furthermore, they challenge the requirement for NRR, which is not imposed by traditional postal services, as such services merely require the recipient to sign a receipt token, confirming the receipt of an envelope, which might be empty as well. A more concrete approach has been undertaken by Tauber (2011), who analyzed existing CeMS systems and reports on the features they provide. His survey shows that most CeMS providers consider NRO as an optional feature, while their systems either provide NRR *or* NRS + NRD evidence. In Slovenia, for example, legislation requires NRO + NRR evidence in certain situations, while in others additional NRS/NRD evidence is mandatory (Paulin and Welzer, 2013, p. 209).

For nm-Gov, NRR is a mandatory feature, as the electronic registries must be able to trust that the response was nondeniably received by the requester. Likewise, requesters must be able to trust that the request was received by the addressed system. To achieve this, it would suffice to automatically respond with a token of receipt that would be nonrepudiably linked

[7] A *message transfer agent* is, for example, an e-mail service provider such as Google or Hotmail.

to the content of the message received. Accordingly, it would be trivial to achieve NRR, if the receiver was unconditionally honest and always confirmed the receipt of the message with, for example, an electronically signed response. However, assuming such honesty in every case would be rather naive, as the sender and receiver might not trust each other and it could be in the receiver's interest to deny the receipt.

A variety of FNR protocols have been developed since the 1990s, which either do involve or do not involve a TTP as mediator between the sender and the receiver of communication. Research in this area has experienced a boost since governments started commissioning CeMS systems as part of their e-Gov agendas. These endeavors have resulted in a multitude of autonomous, mostly closed systems, which are not interoperable (Tauber, 2011; Tauber et al., 2012). This problem is similar to the general unsustainability problem of e-Gov, as criticized in Chapter 4. From the perspective of legislation aimed at removing national borders for the provision of services, such as the European Commission's *Services Directive*, the lack of interoperability of these systems is a significant concern.

A core task of CeMS systems is to achieve fairness, as it "ensures that no party will be in an advantageous position with respect to another one when participating in an exchange of items" (Ferrer-Gomilla et al., 2010). Ferrer-Gomilla et al. (2010) mention five grades of fairness in FNR protocols—strong, weak, true, light, and probabilistic, which they define as follows:

– *Strong fairness*: both sender and recipient receive the expected items (or will receive them in a finite amount of time) or none of them receives what is expected.
– *Weak fairness:* both parties receive the expected items, or, if one party receives the expected items, but the other does not, then the latter can obtain evidence of this situation.
– *Light fairness:* the originator receives NRR and the recipient NRO evidence or none of the parties obtains what they expect.
– *True fairness:* the protocol is *truly* fair if it fulfills the requirement for strong fairness and the evidence generated by an optional TTP would be indistinguishable from evidence generated by the parties themselves.
– *Probabilistic fairness:* the protocol is fair with a probability ε if, and only if, it fulfills strong fairness, or the probability of a cheating party gaining valuable information of its expected items, while the other party gains nothing, is $\geq\varepsilon$.

Initially, probabilistic fairness was regarded as unacceptable by leading researchers in this field and was used as an argument for the necessity of

TTPs. As Tauber's (2011) survey revealed, all then-existing CeMS solutions relied on intermediate TTPs in order to achieve strong fairness. In recent years, however, scholars have recognized the feasibility and utility of probabilistic fairness to serve FNR message exchange in situations in which a TTP is not desired (Ferrer-Gomila et al., 2018; Paulin and Welzer, 2013).

12.3.1 Fair Nonrepudiation Without a Trusted Third Party

It is only logical that commercial CeMS providers insist on acting as a TTP, as this makes it possible to monitor transactions and to bill for the services provided. This practice, however, cannot be applied in nm-Gov, as it would again result in the introduction of another stakeholder as a gatekeeper, and could endanger the integrity of the concept. If we are to omit TTPs, then the only option left is to apply probabilistic fairness, as scholars agree that weak fairness is not acceptable and true fairness is not desired.

At the beginning, probabilistic protocols have been categorically dismissed by Ferrer-Gomilla et al. (2010), as some of them "are not fair and make assumptions like equal computational power among protocol participants."[8] Tauber (2011) has also rejected protocols without TTPs as impractical, noting that "one shortcoming is the fact that these protocols make the assumption of communication partners having the same computational power, which is not realistic." Tauber in his claims referred to Tedrick's (1985) protocol, which relies on a gradual exchange of information, and the Markowitch and Roggeman (1999) protocol, which relies on probabilistic fairness. Feng et al. (2011) also consider gradual exchange to be "not practical."

In their survey of FNR protocols, Kremer et al. (2002) summarize the then-known protocols that did not require a TTP. Early protocols for the fair exchange of secrets, such as Tedrick's (1985) protocol relied on the gradual exchange of bits and required equal computing power on both sides. Such protocols were dismissed by Kremer et al. as unrealistic. Another protocol they describe is the one by Ben-Or et al. (1990), who describe a probabilistic protocol for digital contract signing that involves several rounds of information exchange between the participating parties. During these rounds of interaction the parties increase the probability that the contract under consideration is valid.

[8]In a later study, Ferrer-Gomila et al. (2018) revised their view, accepting the conceptual feasibility of probabilistic protocols as the one described by Paulin and Welzer (2013).

A further protocol noted by Kremer et al. is Han's (1996) protocol in which the sender is in possession of a publicly accessible system *pub*, "which automatically records all the operations (access, modification, …) on the data that it contains." In this protocol, the sender sends an encrypted message to the addressee and publishes the key required to decrypt it on the *pub*. Han's *pub* is essentially a black box which the sender is in possession of. However, this kind of trusted software is generally regarded as being vulnerable to reverse engineering and hacking (Oppliger, 2007; Riordan and Schneier, 1998). Besides, Kremer et al. dispute that Han's protocol is a protocol without TTPs, and suggest that each *pub* is a TTP on its own. However, the reasoning for this position is not further explained and contradicts the common understanding that a TTP is a system that is neither under the sender's nor the receiver's control, but rather under the control of a *third party*.

Riordan and Schneier (1998) proposed the utilization of a neutral public Web forum as a medium for exchanging secrets. In their proposal, the sender symmetrically encrypts the transmitted message and the key is posted publicly on the Web at a specified forum. The address of the forum is chosen by the addressee of the message, who notifies the sender where to post the message to.

Markowitch and Roggeman (1999) and Mitsianis (2001) proposed more elaborate probabilistic protocols, which rely on a gradual exchange of parts of the message. Here, after each received part, the receiver responds with the evidence of a receipt, whereupon the sender sends the next part. If either party aborts the protocol before its completion, neither receives the desired information. However, Kremer et al. note that the probability exists that the addressee could gain the message without sending the last acknowledgment required for the NRR evidence; thus, Markowich and Roggeman admit that "a way for the recipient to receive the message without sending NRR is to guess the number of protocol steps," which is chosen by the originator in secret.

The above-described probabilistic protocols require synchronous involvement of both the originator and the addressee during the execution of the protocol, which is an unrealistic prerequisite for message exchange systems, as this requires both partners to be online at the same time. (This restriction of interaction is not feasible for nm-Gov, simply for the fact that restrictions in the way subjects interact with nm-Gov should be avoided as much as possible.)

Paulin's protocol (Paulin and Welzer, 2013) is a probabilistic protocol for FNR without a TTP that has been designed with the limitations of the Web in mind. This protocol assumes an originator/sender *Alice*, the addressee *Bob*, and an online publicly readable system under Alice's control—the *pub*. The *pub* is a system which should be set up, hosted, and maintained by each originator individually. The *pub* could be a separate software running on the originator's terminal, e.g., mobile phone, or on the originator's modem or Web server, be available as a third-party service, or be part of the services provided by e-mail providers. The *pub* is not a black box and Alice can potentially manipulate it. Even if Alice was able to tamper with the *pub*, it would do no harm to the integrity of the protocol.

The protocol goes as follows. Alice wants to exchange the message M with Bob for NRR evidence; both partners rely on existing PKI, such as X.509. Bob has a cryptographic key pair (private and public key) and both partners know each other's public keys. This protocol does not cover the exchange of keys.

The following steps constitute the information exchange:

1. Alice creates a message M, optionally encrypts it with Bob's public key, resulting in a byte array M_A.
2. Alice chooses two random numbers R1 and R2, whereby R1 must be larger than two.
3. Alice splits M_A into R1 parts of random length and pads each of them with an additional R2 random bytes. R2 is concatenated to the last part of M_A.
4. Alice publishes all but the first part of M_A as a resource on the *pub*, in such way that each resource is identified by the result of a cryptographic hash function over the previous part. Each published resource is logically associated with Bob's identity.
5. Alice sends Bob the message $M2_A$, which contains the first part of M_A, and information about the location of the *pub* and the hash algorithm. $M2_A$ is encrypted with Bob's public key and optionally signed by Alice.
6. Bob receives $M2_A$, calculates the hash of the received first part of M_A, and requests the next part from the *pub*. This is repeated until the *pub* terminates the protocol. Bob must sign each request with his private key.
7. Bob reads R2 from the last part of M_A and cuts the padding from each received part.
8. Bob recomposes M_A and decrypts it with its private key to obtain M.

Each of Bob's request for a part of M_A stored in the *pub* is NRR evidence for the previous part, because the resource's location is revealed only upon calculating the cryptographic hash from the previous part. As each request is signed by Bob and the *pub* is under the control of Alice, Alice is able to collect the requests, and by presenting the collection of the parts of M_A together with the collection of Bob's requests, she can prove to an adjudicator that Bob received M_A.

If Bob stops the protocol before having requested the last part of M_A, then Bob is incapable of reconstructing the message and Alice does not receive full NRR; thus, neither party receives what is expected. The protocol prevents Bob from withholding NRR evidence for the obtained message, as the NRR evidence is logically bound to the message and cryptographically to the collection of all but the last part. This circumstance hypothetically allows Bob to claim that he did not receive the last part despite having requested it, which is a claim that Alice cannot directly disprove through nonrepudiable evidence. However, the protocol allows for the addressee to repeatedly request the last part of the message, which diminishes the risk of technical failure that prevents the receipt of the last part. If, despite repetitive attempts, the addressee still claims to not have received the last part, he could bring this issue before an authority. The authority could then request the missing information from the originator, and in the case that the originator would not deliver it, or delivers information that is not usable, declare the NRR evidence as invalid.

Unlike the Markowitch and Roggeman and Mitsianis protocols, both of which do not prevent the addressee from receiving the message without providing NRR evidence with certain probability, the Paulin protocol bears the risk that the addressee of the transmitted message does not receive (or can claim not to have received) the last part, which is required to decrypt the message. This issue allows addressees to fraudulently claim that they did not receive the final piece of information or that the received information was inapplicable. In such cases, an *authority*—e.g., a court or government agency—is required to resolve the dispute. The authority could force the party that gained the advantage to hand over the missing information or declare the gained nonrepudiation evidence invalid. In both cases, it is reasonable to assume that it is the addressee's responsibility to take immediate action and request that the originator makes the missing information available. If the addressee remains passive, the originator may rightfully assume that the transaction was successful.

12.3.2 The Issue With Conflict Resolution

Until the study by Paulin and Welzer, there was consensus among researchers that TTPs can resolve and/or prevent disputes. Some researchers even claimed that disputes can be resolved "automatically" (Ray et al., 2000).

However, in practice, it is less likely that conflicts caused by fraudulent partners can be resolved without the involvement of an authority. Any kind of conflict resolution before an authority such as a court takes place offline and requires a traditional approach, which can be lengthy. Furthermore, legal precedents in this regard have yet to be formed.

It is not difficult to imagine a fraudulent addressee, who stubbornly refuses to admit to having received a message. Such a person could create a conflict and obstruct solutions that benefit the sender. Even if the certified mail was mediated through a TTP, such a person could claim, for example, that the digital signature on the NRR evidence was produced by somebody else, or that the received message was simply not displayed on their screen. Furthermore, although modern commercial CeMS providers strictly rely on TTPs, a cryptographic connection between the message and the generated evidence (of delivery, receipt, etc.) is generally not provided. Instead, providers such as the Spanish *Certimail*, or the Slovenian *SVEV* system, require the signing of a document, which is only semantically linked to the message that was allegedly sent. Consequently, in case of a dispute, many complex legal questions, including questions regarding the integrity of the TTP, would need to be resolved beforehand.

Once a conflict over the success of a message exchange emerges and is brought before an arbitrator, this conflict can no longer be resolved automatically—it must be resolved in the real world. This defies the purpose of electronic communication, which is mainly about instant exchange of information, regardless of distance. The added value of information processing and automation lies in the possibility of using clear digital structures in systems, without manual intervention. As soon as human intervention is required, the added value of such systems is significantly damaged, if not entirely lost.

Given that no FNR protocol can assure 100% certainty, but rather only *sufficient* certainty in providing the requested evidence, protocols that do not require a TTP can be deemed appropriate to enable nonrepudiable communication when interacting with the nm-Gov electronic registries, as well as for exchanging data between the registries.

REFERENCES

Akram, H., Hoffmann, M., 2008. Supports for identity management in ambient environments—the Hydra Approach. In: 3rd International Conference on Systems and Networks Communications, 2008. ICSNC'08. IEEE, pp. 371–377. https://doi.org/10.1109/ICSNC.2008.77.

Angles, R., Gutierrez, C., 2008. Survey of graph database models. ACM Comput. Surv. 40, 1–39. https://doi.org/10.1145/1322432.1322433.
Bauer, W., 2009. Kryptosysteme basierend auf elliptischen Kurven—Einsatz und Verbreitung in Standardsoftware [Ellyptic-Curve-Based Cryptosystems—Their Use and Acceptance in Standard Software]. A-SIT, Vienna.
Beckett, D., Berners-Lee, T., 2008. Turtle—Terse RDF Triple Language [WWW document]. W3C. http://www.w3.org/TeamSubmission/2008/SUBM-turtle-20080114/. (Accessed 26 December 2011).
Ben-Or, M., Goldreich, O., Micali, S., Rivest, R.L., 1990. A fair protocol for signing contracts. IEEE Trans. Inf. Theory 36, 40–46. https://doi.org/10.1109/18.50372.
Berners-Lee, T., 1998. Relational Databases on the Semantic Web [WWW Document]. DesignIssues. http://www.w3.org/DesignIssues/RDB-RDF.html. (Accessed 26 December 2011).
Berners-Lee, T., 2009. Linked Data [WWW Document]. DesignIssues. http://www.w3.org/DesignIssues/LinkedData.html. (Accessed 26 December 2011).
Berners-Lee, T., Connolly, D., Kagal, L., Scharf, Y., Hendler, J., 2008. N3logic: A logical framework for the world wide web. Theory Pract. Logic Program. 8, 249–269. https://doi.org/10.1017/S1471068407003213.
Bertino, E., Ghinita, G., Kamra, A., 2011. Access Control for Databases: Concepts and Systems. Now, Boston.
Chaudhuri, S., Dutta, T., Sudarshan, S., 2007. Fine grained authorization through predicated grants. IEEE, pp. 1174–1183. https://doi.org/10.1109/ICDE.2007.368976.
Codd, E.F., 1970. A relational model of data for large shared data banks. Commun. ACM 13, 377–387. https://doi.org/10.1145/362384.362685.
Costabello, L., Villata, S., Delaforge, N., Gandon, F., 2012. Ubiquitous access control for SPARQL endpoints: lessons learned and future challenges. In: Proceedings of the 21st International Conference Companion on World Wide Web, WWW'12 Companion. ACM, New York, NY, USA, pp. 487–488. https://doi.org/10.1145/2187980.2188090.
David, B.M., Tonicelli, R., Nascimento, A., Amaral, D., Peotta, L., 2011. Secure Single Sign-On and Web Authentication (No. 2011/246). Cryptology ePrint Archive.
Dodson, B., Sengupta, D., Boneh, D., Lam, M.S., 2010. Secure, consumer-friendly web authentication and payments with a phone. In: Conference on Mobile Computing, Applications, and Services (MobiCASE'10). Santa Clara, CA, USA.
El Maliki, T., Seigneur, J.-M., 2007. A survey of user-centric identity management technologies. In: The International Conference on Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. IEEE, pp. 12–17. https://doi.org/10.1109/SECUREWARE.2007.4385303.
Feng, J., Chen, Y., Summerville, D.H., Hwang, K., 2011. Fair non-repudiation framework for cloud storage: Part II. In: Mahmood, Z., Hill, R. (Eds.), Cloud Computing for Enterprise Architectures. Springer, London, pp. 283–300.
Ferrer-Gomila, J.-L., Hinarejos, M.F., Draper-Gil, G., Huguet-Rotger, L., 2018. Optimistic protocol for certified electronic mail with verifiable TTP. Comput. Stand. Inter. 57, 20–30. https://doi.org/10.1016/j.csi.2017.11.001.
Ferrer-Gomilla, J.L., Onieva, J.A., Payeras, M., Lopez, J., 2010. Certified electronic mail: properties revisited. Comput. Secur. 29, 167–179. https://doi.org/10.1016/j.cose.2009.06.009.
Han, Y., 1996. Investigation of non-repudiation protocols. In: Pieprzyk, J., Seberry, J. (Eds.), Information Security and Privacy. Springer-Verlag, Berlin/Heidelberg, pp. 38–47.
Hayes, J., Gutierrez, C., 2004. Bipartite graphs as intermediate model for RDF. In: McIlraith, S.A., Plexousakis, D., Harmelen, F. (Eds.), The Semantic Web—ISWC 2004. Springer, Berlin, Heidelberg, pp. 47–61.
Hölbl, M., 2009. Development of Identity-Based Authenticated Key Agreement Protocols (Doctoral thesis). University of Maribor, Maribor.

Klemen, M., 2012. Re: crypto problem: validierung XAdES von Bürgerkarte/A-Trust in .NET.
Kremer, S., Markowitch, O., Zhou, J., 2002. An intensive survey of fair non-repudiation protocols. Comput. Commun. 25, 1606–1621. https://doi.org/10.1016/S0140-3664(02)00049-X.
LeFevre, K., Agrawal, R., Ercegovac, V., Ramakrishnan, R., Xu, Y., DeWitt, D., 2004. Limiting disclosure in hippocratic databases. In: Proceedings of the Thirtieth International Conference on Very Large Data Bases—Volume 30, VLDB'04. VLDB Endowment, Toronto, Canada, pp. 108–119.
Markowitch, O., Roggeman, Y., 1999. Probabilistic non-repudiation without trusted third party. In: Proceedings of Second Conference on Security in Communication Networks. Amalfi, Italy.
Miller, J., 2006. Yadis Specification [WWW Document]. Yadis. http://yadis.org/.
Miller, S.P., Neuman, B.C., Schiller, J.I., Saltzer, J.H., 1987. Kerberos authentication and authorization system. In: Project Athena Technical Plan. MIT, Cambridge, MA.
Mitsianis, J., 2001. A New Approach to Enforcing Non-Repudiation of Receipt (Master's thesis). Royal Holloway, University of London.
Oppliger, R., 2007. Providing certified mail services on the internet. IEEE Secur. Priv. 5, 16–22. https://doi.org/10.1109/MSP.2007.15.
Patel-Schneider, P.F., 2010. RDF: Back to the graph. Presented at the W3C Workshop: RDF Next Steps. NCBO, Palo Alto.
Paulin, A., 2015. Towards a Sustainable System for Non-bureaucratic Government: Doctor of Science Thesis (Doctoral thesis). University of Maribor, Maribor.
Paulin, A., Welzer, T., 2013. A universal system for fair non-repudiable certified e-mail without a trusted third party. Comput. Secur. 32, 207–218. https://doi.org/10.1016/j.cose.2012.11.006.
Ray, I., Ray, I., Narasimhamurthi, N., 2000. A fair-exchange e-commerce protocol with automated dispute resolution. In: Thuraisingham, B., Riet, R., Dittrich, K.R., Tari, Z. (Eds.), Proceedings of the IFIP TC11/WG11.3 Fourteenth Annual Working Conference on Database Security: Data and Application Security, Development and Directions. Kluwer Academic Publishers, Boston, pp. 27–38.
Recordon, D., Reed, D., 2006. OpenID 2.0: a platform for user-centric identity management. In: Proceedings of the Second ACM Workshop on Digital Identity Management, DIM '06. ACM, New York, NY, USA, pp. 11–16. https://doi.org/10.1145/1179529.1179532.
Riordan, J., Schneier, B., 1998. A certified e-mail protocol. Presented at the 13th Annual Computer Security Applications Conference. ACM Press.
Seaborne, A., Manjunath, G., Bizer, C., Breslin, J., Das, S., Davis, I., Harris, S., Idehen, K., Corby, O., Kjernsmo, K., et al., 2008. SPARQL/Update: A Language for Updating RDF Graphs. W3C Member Submission, p. 15.
Tauber, A., 2011. A survey of certified mail systems provided on the internet. Comput. Secur. 30, 464–485. https://doi.org/10.1016/j.cose.2011.05.001.
Tauber, A., Apitzsch, J., Boldrin, L., 2012. An interoperability standard for certified mail systems. Comput. Stand. Inter. 34, 452–466. https://doi.org/10.1016/j.csi.2012.03.002.
Tedrick, T., 1985. Fair exchange of secrets. In: Proceedings of CRYPTO 84 on Advances in Cryptology. Springer-Verlag, Inc., New York, NY, pp. 434–438.
Vicknair, C., Macias, M., Zhao, Z., Nan, X., Chen, Y., Wilkins, D., 2010. A comparison of a graph database and a relational database: a data provenance perspective. In: Proceedings of the 48th Annual Southeast Regional Conference, ACM SE'10. ACM, New York, NY, USA, pp. 42:1–42:6. https://doi.org/10.1145/1900008.1900067.
Zhou, J., Gollman, D., 1996. A fair non-repudiation protocol. In: IEEE Symposium on Security and Privacy, 1996—Proceedings IEEE, pp. 55–61. https://doi.org/10.1109/SECPRI.1996.502669.

CHAPTER 13

Describing Legal Rules Through a System of Electronic Legal Acts

Contents

Chapter 12 dealt with the major technological challenges in designing nm-Gov registries—technologies for storing and querying data and technologies for assuring fair nonrepudiation of exchanged messages in the interaction with the nm-Gov registries. This chapter deals with the third major challenge, that is, the question of how to enforce policies that govern the access to the stored data.

In the nm-Gov model, the access control policies are described by the concept of constellation-based reasoning (CBR), inspired by the pin-tumbler lock in which a key can open a lock only if the cuts in the key can push the pins in the lock to the required position. Unlike in the physical pin-tumbler lock, where the constellation of pins has been fixed by design, the "pins" and "cuts" in nm-Gov's metaphorical locks are the core data stored in the system and the access control policies, both of which transform as time goes by.

If we picture the nm-Gov registry as an advanced relational database, then the informatized structures in that registry are the following: core *data*; *rules* governing how this data is read, written, and modified; and the *structure*, within which the data is stored. The *data* are the core informatized assertions, such as one's name, one's address, one's high school diploma, one's university degree, and the reference to one's spouse. The *rules* are the *locks* from CBR, from Section 9.2, that govern the core data: a student cannot create their own university degree, but this will be created by a university once the

Smart City Governance
https://doi.org/10.1016/B978-0-12-816224-8.00013-3

student has passed all the formalities; likewise, a town's new mayor will be registered through the formal procedures that involved their election. The *rules* will thus contain the conditions that must be fulfilled (i.e., the required constellations of *core data*) so that the core data can be created or changed. The *structure* is the semantics and the form in which the data is stored. In the land registry sample depicted in Section 12.1, the structure was given as fields {`subject_id`, `legal_relation`, `land_parcel_id`}.

These elements of the electronic registries are then the law (law as architecture) that governs the public apparatus in informatized governance. If these elements make up the law, then it is of utmost importance that the rules and the structure *can* be scrutinized publicly—if permitted to do so by those who have designed the rules. Furthermore, it is imperative that these elements can be created, changed, or modified through collective decision-making, which itself is governed by this very same system of rules.

This chapter provides a summary of an instantiation of a prototype-level nm-Gov registry, where the CBR principle is implemented to an extent which allows nonmediated governance of data, structure, and access control rules (Paulin, 2015). The concretization of this registry was called the *Secure SQL Server* (SecSQL), and the system of access control policies was named the system of *Electronic Legal Acts* (ELAs).[1] SecSQL relied on SQL as the artificial language for CRUD queries and the MySQL relational database as the system for storing data. The ELA system therefore utilized query rewriting as a means to achieve fine-grained access control to govern the data stored in the nm-Gov registries.

This chapter is organized as follows: Section 13.1 discusses how *dynamic* fine-grained access control (*d*FGAC) was deployed in SecSQL to enable *timelessness* and *genericness* of the system. Section 13.2 describes the core architecture of the SecSQL prototype, thus providing a reference architecture for nm-Gov registries. Section 13.3 provides examples of how the ELA system enables noninterpretative application of law in the SecSQL system, using the power of the SQL language.

[1]The term ELA is used to refer to a concrete instantiation of the CBR principle as used in SecSQL. SecSQL on the other hand is a concrete instantiation of an nm-Gov registry. This distinction allows a separation of concerns in research by leaving CBR and nm-Gov to describe artifacts on the level of models, while ELA and SecSQL refer to the concrete prototype instantiations used in the case summarized here.

13.1 DYNAMIC FINE-GRAINED ACCESS CONTROL (*d*FGAC)

Fine-grained access control (FGAC) of data in nm-Gov registries must cater to an environment in which collective action can change the access control policies in a way that cannot be predicted at design time. Therefore, the registries must be designed in such a way that they can apply unpredictable rules to unforeseeable requests, without restricting the meaning of either. To make this possible, access control policies must be able to regulate access to each attribute within a tuple independently. In Section 12.1.1, three options for fine-grained data access control have been noted: query rewriting, extension of the SQL specifications, and transparent authorization views. Extending the SQL specification to accommodate for FGAC would be a welcomed option, but this would require substantial further research and exceeds the scope of this treatise. This leaves us with the other two options to discuss further.

Authorization views would be unfeasible for nm-Gov, as this technique relies on prefabricated views (stored queries that define subsets of the data stored in a database), which would need to be created in advance. This would again result in hard-coded policies, as it is the case with modern e-Gov applications, except that the access control logic would now reside inside the DBMS instead of being part of the processing logic of the application.

Query rewriting in the way as suggested by LeFevre et al. (in Bertino et al., 2011) would not be feasible either. Their approach implied a rigid structure of metadata, which described for each tuple about a subject (a patient, in their case) the specific conditions under which a given part of the data could be accessed by a given requester. Thus, the freedom of access to data would be limited by a number of predefined use cases, and so is fundamentally incompatible with the *unpredictability principle* of nm-Gov. Commercially available implementations of query rewriting, such as the *Virtual Private Database* (VPD) from Oracle, as described by Bertino et al., are also unfit to cater to the unpredictability principle. As VPD governs data access through internal functions which can be linked to tuples, it is implied that the procedural logic inside these functions has a scope which requires that the future use of the data is known in advance.

An implied condition of nm-Gov is that the creation and enactment of access control policies must be subject to collective decision-making. Therefore, the following possibilities must be provided:

1. A member of the decision-making body must be able to propose the creation, change, or deletion of rules or structures without enacting such a proposal, in accordance with existing policies.

2. The decision-making body must be able to collectively accept a proposal in accordance with existing policies.
3. It must be possible to enact a collectively accepted proposal in accordance with existing policies.

None of the approaches summarized by Bertino et al. is able to cope with these requirements, as any existing approach requires an *administrator* to implement authorization policies in one way or another. nm-Gov registries on the other hand must be able to undergo arbitrary changes during runtime without the intervention of human administrators in order to stay true to the concept of nm-Gov.

Both the relational calculus on which relational databases are based and the CBR mechanism that was presented in Section 9.2 have their roots in relational algebra. The CBR mechanism as implemented in SecSQL also relied on relational algebra. More specifically, it used *cascading projections* (cascading subsets of data) to render an ad hoc set of the data to which the requester was allowed access. The requested action was then performed over this subset of data. In this method (Fig. 13.1), the access restrictions/rules were applied one after another so that the originally requested operation was conducted over the final view after all projections have been applied.

This approach allows us to apply a virtually unlimited number of rules to the incoming request. Each of these rules would govern access to a

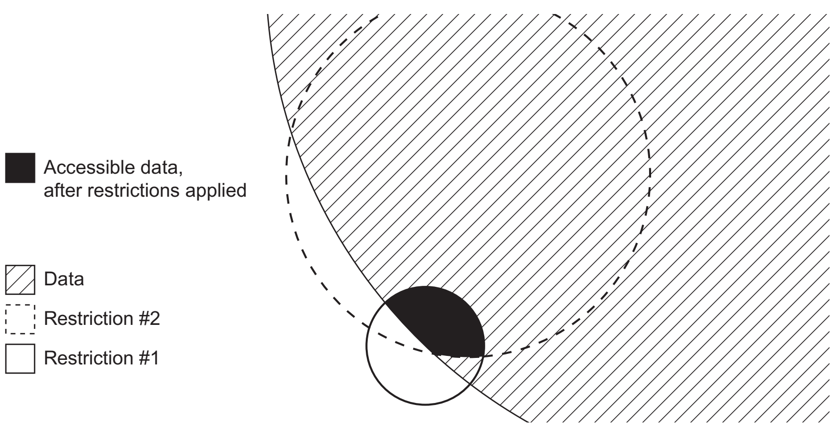

Fig. 13.1 Through cascading projections (subsets) that are defined by the requested query, an ad hoc context-dependent virtual view of the accessible data is rendered, over which the original query is executed. This way bespoke dynamic fine-grained data access control is exercised.

certain element of the data or structure stored in the database. The set of rules to be applied to rewrite the incoming query would thus depend on the elements addressed by the query—the set of rules is implicitly bespoke for each unique query. The custom set of rules to be applied would be dependent on the addressed fields, and on the type of access requested. As each rule has full power over which subset of data to reveal, it is possible to fine-tune access to individual fields based on complex conditions such as existing constellations of data stored in other parts of the database. The relational database allows the rules themselves to be stored in the form of data. Accordingly, these rules can be added, modified, or removed just as any other kind of data; these modifications would be governed by existing access control policies.

By this technique, the overall access control policies that govern a specific request for access to data would be composed of a bespoke set of rules. Accordingly, the *access control policies* as such are not explicitly stored within the logic of the database management system, instead access control is defined through implied constellations of stored data. For example, a law enforcement agent could be eligible to access data belonging to a person under prosecution only between specific office hours, within a specific period of time, and given that the case is still pending investigation. This rule would then require knowledge of the context (who is the accessor, what time is it?), as well as other data stored within the system, such as whether or not the case is still open.

FGAC is an established technique that enables advanced features such as geo-fencing, an approach where access to a resource is conditional based on the geographical position of the requester. While established FGAC mechanisms focus on providing specific utility to a predictable context, as in the case of geo-fencing, the type of FGAC required to realize nm-Gov registries is more complex, since the context is not known in advance. As the context is *dynamic*, rather than predetermined, the FGAC technique as adapted in SecSQL was named *dynamic fine-grained access control*—*d*FGAC. In this capacity, *d*FGAC has been designed as a general-purpose technology (GPT), which can serve as a mechanism for generic access control to resources.[2]

[2]An example of industrial application of *d*FGAC has been reported by Paulin and Thuemmler (2016) in the domain of governing access to Hippocratic data and supply-chain management.

13.2 ARCHITECTURE OF THE NM-GOV REGISTRY

The interaction with the nm-Gov registry as instantiated in the SecSQL system involved the exchange of electronically signed SQL queries, which were sent over the Web to the endpoint of the registry. Upon processing the SQL query, the registry responded with a result set according to what has been requested.

The SecSQL instance was comprised of the following logical modules:

(1) The front-end module provided the northbound API and listened to the endpoint for requests over HTTP. The front-end module orchestrated the operation of the back-end modules and provided them with the information that described the context, such as the location of the request, the time of the request, and the identity of the requester.

(2) A crypto module in the back-end was responsible for verifying message integrity and signature validation. This module further extracted the identity of the requester and provided an identity token for use in the context of the request.

(3) An ELA module in the back-end analyzed the request query and retrieved request-related ELAs from the available ELA repositories.

(4) The FGAC module provided *d*FGAC functionality based on the applicable ELAs, taking into account the context of the request. This module interfaced with the SQL interface of the database to which it passed the rewritten request query.

(5) The back-end database stored the data which could be queried through a standard SQL interface.

The requester first formulated the request in the form of SQL statements, electronically signed it and conveyed it to the endpoint of the SecSQL system, and then waited for a response. The SecSQL system delegated the received message first to the crypto module, which checked the integrity of the message and extracted the identity of the requester. Next, the validity of the requested SQL statements was checked, and if the request was valid, contextual information about the request—identity of the requester and the requested query—was passed to the ELA-rules engine. The rules engine retrieved the set of access control policies that applied to the requested query and the context of the request. These rules and the original query were then delegated to the FGAC module to rewrite the incoming query so that it incorporated the access control rules that governed the request. The rules engine then passed the thus rewritten query to the back-end database for execution. The query result was finally passed back through the call chain and responded to the requester.

Requesters were free to design whatever SQL queries they liked. Such queries might have consisted of many SQL statements and some of them might even be malicious SQL injection attempts intended to harm the system. The SecSQL system did not attempt to prevent this, as it would contradict the implied *neutrality principle* of nm-Gov, which mandates that *any* request (even bogus and malicious ones) must be treated equally. Hypothetically, it might be reasonable for the server to limit itself to accepting only requests digitally signed by identities issued by certain identity providers in order to assure that only existing members of a society would issue requests to the registries.

13.2.1 The SecSQL Prototype

The SecSQL prototype instantiation of an nm-Gov registry was built as a Web application and hosted in a commercial Web server to provide accessibility via the Internet. The system processed the requests as depicted in Fig. 13.2. Once an electronically signed SQL statement was received, the system verified its integrity and extracted the identity of the signer, after which it nondiscriminatorily rewrote the SQL statement by applying

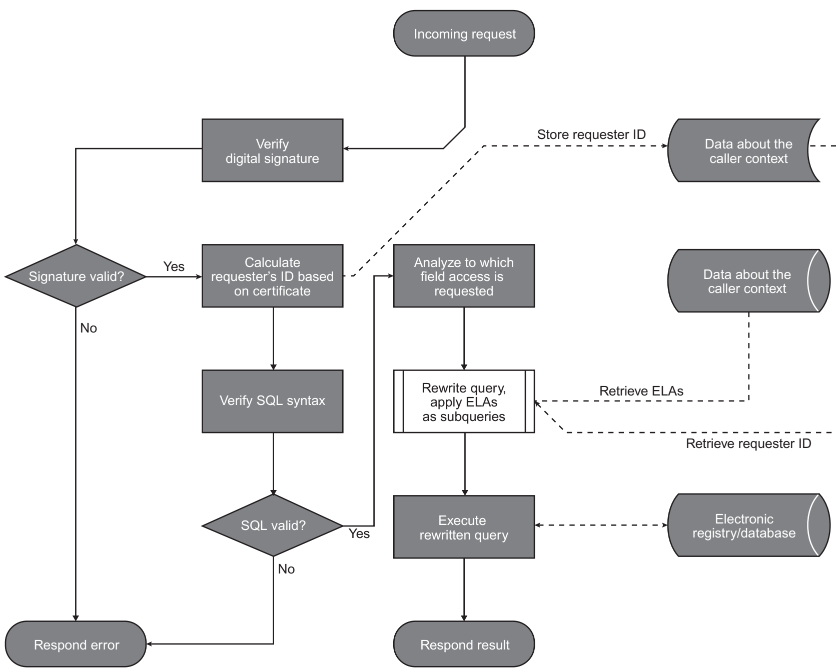

Fig. 13.2 Execution diagram of the SecSQL prototype.

rules from the ELAs in the form of subqueries. Finally, it executed the thus rewritten queries against the database. To facilitate user interaction, a user-friendly graphic user interface was provided, allowing users to compose SQL queries and visualize the results responded by the server.

The prototype accepted requests packed in a custom JSON structure, as shown in Table 13.1. The field `SQL` contains the plaintext SQL query, as designed by the user; field `Pkcs7` contains a Base64 encoded digital signature of the SQL query, assuring the integrity and nonrepudiability of the SQL query, as well as conveying the applicant's identity to the server; field `Comment` exists to accommodate additional natural language comments for documentation purposes, and has had no impact on how the system processes the request.

Each request received by the prototype was initially delegated to the crypto module to check its integrity and validate the digital signature. Each signed request came with an X.509 certificate, from which the requester's identity was extracted. This was done by calculating an SHA-256 hash, serialized as a Base64 string, and then used to internally identify the requester. This identifier was made available as a variable in the rewritten SQL statement, from where it could be used by the ELA policies. Table 13.2 shows the structure of the response returned by the prototype.

Table 13.1 JSON structure of the request

```
{
   SQL:       /* content of the request expressed in SQL */,
   Pkcs7:     /* Base64 encoded Pkcs7 signature of the SQL */,
   Comment:   /* informative human-legible description of the request */
}
```

Table 13.2 JSON structure of the response

```
{
   Results:
   [{
      ExecutedSQL:     /* the transformed request */,
      RequestedSQL:    /* the original request */,
      Rows:
      [{
         Name:         /* the name of the column/attribute */,
         Value:        /* the stored value */
      }]
   }],
   Feedback:           /* feedback message, e.g. in case of error */,
   GenerationDate:     /* execution date */,
   OK:                 /* flag denoting success of the execution */
}
```

13.3 NONINTERPRETATIVE APPLICATION OF ELECTRONIC LAW

The ELA system within the SecSQL instance has been realized based on a set of proposable and enactable policy documents, which together form a system of data-access *privileges* and *restrictions*, based on the principles of *d*FGAC as described in Section 13.1. The main challenge in realizing the ELA system is that the *unpredictability principle* also applies to the ELA rules themselves—they can be created, changed, or removed just like any other kind of data. Accordingly, the ELA system was applied in a circular manner, as valid ELA policies regulate how to create new, or modify existing, ELAs.

The ELA system regulated access based on *explicit* access permissions and restrictions to access data. If not explicitly granted, access to data has been denied by default, but if access was granted, it *might* have been moderated through restrictions. This means that by default all data was locked away, the exception being only the metadata about the structure of the data itself.

Requested SQL queries were delegated to the ELA module, which first analyzed their syntactical validity. Next, it extracted information about the scope of access—i.e., to which relations and attributes access is requested and of what type the statement is (e.g., a SQL `SELECT, INSERT, UPDATE`). Based on the request type of the query and the affected attributes, the corresponding ELA rules were retrieved from the policy repository, whereupon the incoming query was rewritten so that the applicable ELA rules constrained the set of data over which the query was executed, as illustrated by Fig. 13.1.

In the case that a `SELECT` query was requested, the registry verified that the requester had explicit permissions to read *each* of the requested attributes. In case the all-attributes wildcard `(SELECT *)` was requested, permission to access all attributes by means of the asterisk wildcard must have been *explicitly* granted. In the case that access to at least one of the requested attributes has not been granted, the entire request was denied. This prevented data to be revealed only partially—a circumstance which is referred to as the *Truman model* (Rizvi et al. in: Bertino et al., 2011, pp. 82–83), named after the 1998 movie *The Truman Show* in which a reality TV show is streaming the real life of a person living in his fake town. Access to attributes would usually be granted conditionally—e.g., information about government employees may only be revealed to employees who are in service. This condition can be expressed through an appropriate ELA rule, which would be applied to the incoming query.

Table 13.3 Sample transformation of an INSERT request

```
1  INSERT INTO sandbox (name, toy) VALUES (‘Loys’, ‘ball’);
-------------------------------------------------------------------
2  WHERE @toy IN
3  (SELECT t.toy FROM toys t
4     WHERE t.ageLimit < (SELECT c.age FROM children c WHERE c.name = @name));
-------------------------------------------------------------------
5  SET @name = ‘Loys’;
6  SET @toy = ‘ball’;
7
8  INSERT INTO sandbox (name, toy)
9  SELECT @name, @toy
10 FROM DUAL
11 WHERE @toy IN (
12    SELECT t.toy FROM toys t
13       WHERE t.ageLimit < (SELECT c.age FROM children c WHERE c.name = @name)
14    )
```

The original request (line 1) is transformed into a realized request (lines 5–14) based on a subquery from a relevant ELA (lines 2–4).

In case of write access (`INSERT`, `UPDATE`), the system first verified that the appropriate regulations had been assigned, just as in the case of the request of read access (`SELECT`). In case of an `INSERT` query, each attribute was extracted and defined as a variable, as shown in Table 13.3—the variables are defined in lines 5 and 6. In this way, it was possible to fully control the content of the assigned value, which could hypothetically be a query of its own. Next, the insert statement was fully reconstructed and executed against a `DUAL` virtual relation, a dummy relation used to enable otherwise unsupported actions.[3] This dummy relation allowed for an inclusion of the variables as extracted from the original query, which could be accessed from within the ELAs that were applied in the form of `WHERE` clauses to the `DUAL` relation.

13.3.1 Virtual Function SX.ENACT

In order to enact a collectively chosen new policy, a dedicated function had to be introduced, to allow accepted ELA proposals to be enacted in accordance with existing ELA policies. This function was named `SX.ENACT`,

[3] According to Web sources, it was Chuck Weiss who implemented DUAL into the Oracle database "as an underlying object in the Oracle Data Dictionary. It was never meant to be seen itself, but instead used inside a view that was expected to be queried. The idea was that you could do a JOIN to the DUAL table and create two rows in the result for every one row in your table. Then, by using GROUP BY, the resulting join could be summarized to show the amount of storage for the DATA extent and for the INDEX extent(s). The name, DUAL, seemed apt for the process of creating a pair of rows from just one" (Weiss, 2002).

and it accepted two mandatory parameters—`@id` and `@statement_loco`. The parameter `@id` contained the identifier of the tuple that contained the ELA to be enacted. The parameter `@statement_loco` accepted a single `SELECT` statement, to define the location of the proposal within the database.

`SX.ENACT` utilized MySQL's *prepared statements* functionality, allowing arbitrary SQL statements to be triggered through SQL commands. The SecSQL prototype enabled users to temporarily store arbitrary SQL statements in the form of textual data at any arbitrary location in the database. Such textual data could then be enacted under the conditions imposed by existing ELAs, and accordingly could be turned into new ELAs, new databases, or alterations of existing ones. Table 13.4 shows an example of a statement that is to be enacted and how the statement has been rewritten before execution.

Using this function, it was possible to govern collectively legitimized creation and alteration of tables, and to set/modify rules. The function did not prevent malicious commands to be executed, as it lacked the means to supervise the content of the query. This lack of control was partially deliberate, to prevent the system from restricting the intended actions of its users. This freedom, however, would have enabled legislative bodies to accept and enact a command that would wipe out all jural data of the informatized society, and thus effectively throw society into total chaos.

Table 13.4 Sample SQL call to the virtual function SX.ENACT before (above) and after (below) query rewriting

```
1   SET @id = "SOP91-01-1094";
2   SET @statement_loco = "SELECT cmd FROM proposals WHERE id = '91-01-1094'";
3
4   CALL SX.ENACT(@id, @statement_loco);
--------------------------------------------------------------------------------
5   SET @sx_pid = "SOP91-01-1094";
6   SET @sx_act = (SELECT command FROM proposals WHERE id = '91-01-1094');
7   SET @sx_res = (SELECT @sx_act FROM DUAL WHERE @sx_pid IN
8      (
9         SELECT p.id
10        FROM proposals p
11        WHERE
12           (SELECT COUNT(*) FROM legislator.members) =
13           (SELECT COUNT(*) FROM legislator.decisions d
14              WHERE d.id = @sx_pid AND d.decision = 'in favor')
15     )
16  );
17
18  PREPARE sx_res FROM @sx_res;
19  EXECUTE sx_res;
20  SELECT true;
```

The case shown demonstrates the enactment of a command with the ID "SOP91-01-1094" for which full consensus in the legislative body must have been reached—hence the number of votes in favor must equal the number of members of this body. The WHERE clause (lines 11–14) is from the ELA which governs the read access to the data in the table proposals.

13.3.2 Liquid-Democratic Decision-Making Through ELAs

The implication of nm-Gov that *any* kind of societal system must be model-able by means of the ELA system has been put to the test with liquid-democratic decision-making (LD). LD has been described in Section 3.5.1 as a system of delegating power within a network of people, whereby any member of this network can delegate their power (their own share, plus all received power) to another member, while remaining able to revoke their delegation at any time. The result of this is a fluid (hence, "liquid") network of trust, in which individual nodes (members) hold significant shares of societal power, while the majority has delegated away their votes and remain passive followers until activated. LD breaks the constraints of traditional delegated decision-making, which require bodies of representatives to make decisions, or carry them out, and opens up possibilities for substantially different paradigms of social function delivery.

LD thus ultimately informatizes what is crucial to social systems, namely trust and societally administered legitimacy. This feature makes LD a core enabler for collective decision-making that does not require human agents for the moderation of the process. Unlike in the context of party politics, where LD is used for opinion gathering and the shaping of the party line (see the case of the German Pirates described in Section 3.5.2), in nm-Gov, LD can be utilized to enact ELAs (the CBR locks) and thus regulate the conditions under which individuals can assume and exercise eligibilities. The rules of the LD process can again—at least in theory—be appropriately tuned to fit different collective decision-making scenarios. And these same rules can again be regulated by means of CBR locks, yielding a morph-able system in which the transition from one form of governance to another can be regulated *within* the system itself.

Since the ELA system utilizes SQL as the universal artificial language to query data in relational databases, it utilizes projections (subsets) as a way of defining restrictions to access the data. If in this setting LD is to be used for collective decision-making, one needs to be able to determine the majority in a collective decision-making context, so as to be able to *enact* the collective decisions according to their preferences. A rule, which would restrict the desired action by requiring prior consent from the majority of members, must accordingly be designed in the form of a projection.

In order to calculate a majority in LD, the entire network of transitive delegations of power must be traversed and the might of the requester's individual network in the particular context must be calculated ad hoc. Let us assume that each individual can delegate at any time their vote to *anybody*, with the delegation carried out silently without notifying the delegate. This then requires a recursive query over a table which holds the information on who delegated their vote to whom.

Table 13.5 shows how a recursive query would determine whether or not a particular person holds a majority of power in the LD network at a given moment. This example assumes the existence of two tables: table `members{member_id,proxy}` holds the information on the subjects of the particular society, as well as the information of whom individuals have delegated their vote to (if they have done so at all); table `votes{member_id,vote}` holds the individually expressed votes of the particular members. The information about the power of each individual member is calculated ad hoc by means of the common table expression (CTE) `my_followers`. This CTE is shown in lines 7–20 in Table 13.5. It recursively traverses all nodes (the individuals of the LD network) that link to the node for which the cumulative power is inquired. While traversing the network, all individuals who expressed their preference in table `votes` are excluded from the calculation of the cumulative power (line 14). Cyclical delegation of power is prevented during the calculation (line 15)—this would occur if two individuals would delegate their power to each other.

The result of this query about one's power within the LD network could be used as part of another CBR lock/ELA policy. This mechanism could be used to, e.g., mandate that a communal decision can be enacted

Table 13.5 SQL query to determine a given individual's power at the moment of calculation using Liquid Democracy

```
1  DROP TABLE IF EXISTS vars;
2  CREATE TEMP TABLE vars(id TEXT);
3  INSERT INTO VARS (id) VALUES (“Loys”);  // id of individual whose might
4                                          // we want to calculate
5                                          // (to be provided by the context)
6  WITH RECURSIVE
7     my_followers(name, level) AS
8     (
9        VALUES ((SELECT id FROM vars LIMIT 1), 0)
10       UNION ALL
11       SELECT m2.member_id, my_followers.level + 1 FROM
12       (
13          SELECT * FROM members m
14          WHERE m.member_id NOT IN (SELECT v.member_id FROM votes v)
15          AND m.member_id NOT IN (SELECT id FROM vars LIMIT 1)
16       )
17       AS m2
18       JOIN my_followers ON m2.proxy = my_followers.name
19       ORDER BY 2 DESC
20    )
21
22 SELECT (COUNT(*)*100/(SELECT COUNT(*) FROM members)) || ‘%’ AS my_might
23    FROM my_followers;
```

only by an individual (or a collective of individuals), who holds at the given moment at least 51% of the power within the society.

The mechanism from Table 13.5 could be further fine-tuned to allow for a more elaborate regulation of collective decision-making. For example, rules could be set in place to regulate under which conditions an individual could cast a vote preference into the table `votes`, and under which conditions a delegation/revocation of power to a fellow member of the community could be registered in the table `members`.

REFERENCES

Bertino, E., Ghinita, G., Kamra, A., 2011. Access Control for Databases: Concepts and Systems. Now, Boston.

Paulin, A., 2015. Towards a Sustainable System for Non-bureaucratic Government: Doctor of Science Thesis (Doctoral thesis). University of Maribor, Maribor.

Paulin, A., Thuemmler, C., 2016. Dynamic Fine-Grained Access Control in e-Health Using the Secure SQL Server System as an Enabler of the Future Internet. IEEE, pp. 1–4. https://doi.org/10.1109/HealthCom.2016.7749462.

Weiss, C., 2002. The History of Dual. http://web.archive.org/web/20041205061859/http://www.oracle.com/technology/oramag/oracle/02-jan/o12sendmail.html. (Accessed 26 August 2018).

CHAPTER 14

Applied Nonmediated Governance: Common Scenarios

Contents

Nonmediated governance (nm-Gov) would radically change how one's legally relevant allowed behavior is determined. In traditional, mediated governance, one's legal eligibilities are asserted and demonstrated through tokens such as documents, ID cards, and certificates. In nm-Gov, however, eligibilities are *determined* by querying the system of nm-Gov registries, such that any particular eligibility is determined ad hoc based on the constellations of stored core data. This shift from *declaring/asserting* eligibilities to *determining* them from data opens up new yet to be explored avenues. In nm-Gov, essential human characteristics such as fallibility, incompetence, laziness, and corruptibility are reduced to a bare minimum—humans would only play a role in producing the core assertions and in executing eligibilities in the real world.

Informatizing governance establishes a radically new channel of control through technology; moreover, it enables the public apparatus to be analyzed through technology. Today, it is virtually impossible to scale and measure the size of the modern public apparatus—i.e., we can't precisely state which individuals and organizations are part of it, what function they provide to society, and how the members or the public apparatus influence each other. One can put this statement to the test by trying to collect information

https://doi.org/10.1016/B978-0-12-816224-8.00014-5

about all subjects (both natural and legal ones) who receive funding through public authorities. Hypothetically, this would imply addressing *all* public law organizations and requesting information about whom they distribute public funds to. While this would be a most interesting and revealing endeavor (it would shed light on the networks that make up the public apparatus), this task would soon become stalled in the myriad of jural quagmires, appeals, and court proceedings. An example of one such investigation that became trapped in the jural quagmires was the case of the freedom-of-information request described in Section 1.3.3, in which the highest level of legal institutions in Slovenia put up a legal fight to prevent their own data from being disclosed.

This paradigm shift reveals several new opportunities. There is significant political opportunity that can be seized by new networks of power in order to portray themselves as reformers ringing in a brighter future for citizens. Economic growth can be boosted by the research and development of new technologies for governance informatization. This would give new work to researchers and scientists, system developers, and technology evangelists, and would yield the emergence of new technological ecosystems, and so on. Furthermore, there is hope that informatized governance can stimulate the discovery and development of new social functions, which are not able to be hosted by modern models of governance. More specifically, the shift toward a clear technical system for societal governance that can be interacted with in standardized means through technical interfaces and digital communication enables never-before possible opportunities, much like the Internet enabled the invention of entirely new possibilities which before were simply unthinkable.

In order to prove the conceptual feasibility of nm-Gov, this new concept has to demonstrate that it can handle all of the same situations that contemporary governance does. This is what this chapter aims to do: to demonstrate how nm-Gov is capable of providing existing functions of the public apparatus based on examples from the real world. To this end, Section 14.1 discusses the transformation of an administrative procedure, taking the case of acquiring a residence and work permit as described in Section 1.3.4 as the point of departure. Section 14.2 looks at how decision-making of modern parliaments could be carried out if placed on an nm-Gov platform. Section 14.3 discusses public funding and taxation, and Section 14.4 discusses the case of open government data as described in Section 2.1.4. An idea for a novel form of public funding and taxation enabled by nm-Gov and Liquid Democracy—the *Quantum Budget (QB)*, is outlined in Section 14.5.

14.1 SCENARIO ONE: THE RESIDENCE AND WORK PERMIT

People who wish to live and earn a living in a foreign country are required to obtain the right to do so from the host state. In order to get access to the labor market, they must obtain a residency and work permit through an administrative procedure. In Section 1.3.4, we illustrated such an administrative procedure in which the applicant was requesting a *Rot-Weiss-Rot Karte* (RWR-K), Austria's residence and work permit awarded to migrants with top qualifications. In Section 1.3.4, our focus was on the sluggishness of the lower officials who handled the case and the bad impression this left of the state. This section analyzes how nm-Gov could make such proceedings better.

The conditions to become eligible to work and live in Austria are regulated by the *Settlement and Residence Act* (NAG) and the *Employment of Foreign Nationals Act* (AuslBG). The AuslBG mandates that a non-Austrian national can be employed in Austria only if the employer acquires permission to employ the foreigner, or if the foreigner acquires permission that grants them the right to be employed. Such permission can be acquired only if the candidate has a right to reside in Austria, in accordance with the NAG. Aside from this, fulfillment of further conditions, such as the assurance of the employer to respect employment laws and a clean history of conduct of both employer and employee in this regard, are required.

Foreigners with high qualifications receive the work and residence permit through the RWR-K. As general requirements, the applicant has to prove to have adequate accommodation available and health insurance covering services in Austria. Aside from this, the right to reside in the country can only be granted if this would not severely influence relations of Austria with some other country, etc.

The application for the RWR-K has to be submitted to the responsible agency as defined in the NAG, in addition to a written statement from the future employer stating that the employment conditions as given in the application will be fulfilled. The receiving agency is supposed to immediately reject the application in case it is incomplete or if the applicant has been banned from residing in Austria. If there is no reason to reject the application, the receiving agency must immediately delegate the application to the *Public Employment Service Austria* (AMS, a national agency responsible for job seekers), which must hear the *regional advisory board* on the matter, and confirm within 4 weeks whether or not the conditions for granting the application are fulfilled. If the decision of the AMS is positive, the regionally responsible agency grants the RWR-K and issues a tangible ID card.

The right to live and work in Austria thus is established if the applicant can provide evidence that prove a set of defined criteria, and if the *regional advisory board* does not object. Fig. 14.1 shows the schematic process of how Austrian authorities decide on granting/denying the right to live and work in Austria. The processes and decision points that do not require discretionary power in decision-making are depicted as filled elements—these processes/decisions could be automatized into an e-Gov system. To handle the process, at least three stakeholders are involved: the *agency* responsible for deciding on the request, the *AMS*, and the *advisory board* of the AMS, two of which (the agency and the AMS) are bound to a strict bureaucratic protocol.

How would obtaining the eligibility to live and work look in nm-Gov Austria? For one, there would be no one to refuse or reject an application, as there would be no *application*, nor any bureaucratic procedure. In accordance with the key:lock paradigm of constellation-based reasoning (CBR), the applicant themselves would forge, piece-by-piece, the required key to unlock their desired eligibility. Accordingly, they might still require

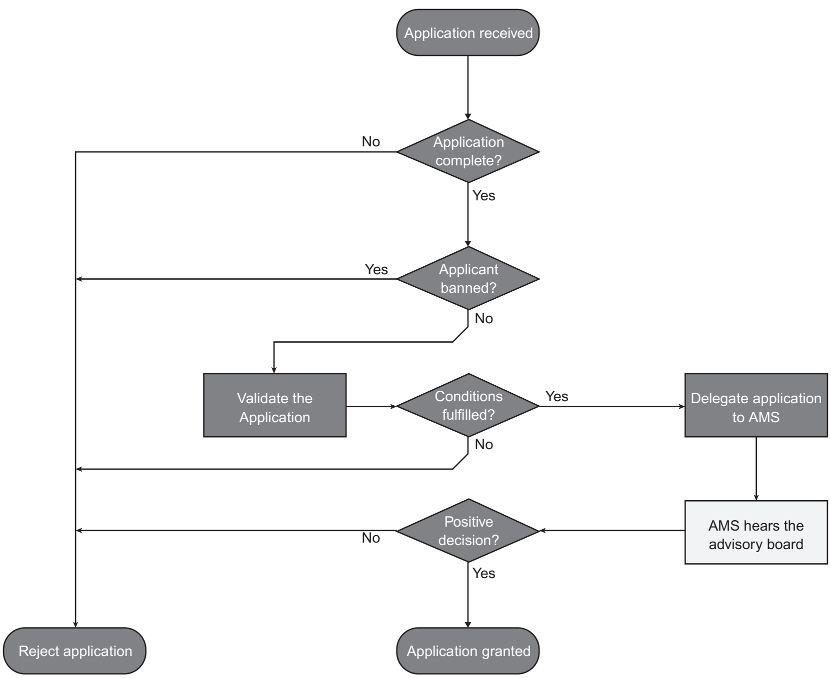

Fig. 14.1 Process-oriented decision-making—application for Rot-Weiss-Rot Karte (simplified for illustration).

the exact same evidence as before—confirmations from educational institutions on the level of education, proof of having secured accommodation, a secured job contract from an organization with a clear history of conduct, etc. Unlike in the bureaucratic context, where the bureaucracy routes the application to be heard by *AMS' advisory board* (Section 1.3.4 provided an example of how unnecessarily long that can take), in nm-Gov, the subjects themselves undertake the actions required to create the right constellation of jural data that *unlocks* the desired eligibility—thus, in nm-Gov, it would be up to the applicant themselves to request the required confirmation from *AMS' advisory board*.

Once all the data is organized in the correct constellation, the applicant would automatically have the desired rights to legitimately live and work at the chosen destination. These rights remain upheld until the point at which there is some change in the nm-Gov registry that alters the requirements for the CBR lock or invalidates the previously functioning CBR keys. This could happen if, for example, a severe penalty against the foreigner became legally binding. Fig. 14.2 depicts how residence and work permission could be determined through CBR.

From a technical perspective, several electronic registries would be required to hold the informatized data on housing contracts, job contracts, education, etc. National and foreign educational organizations could either directly provide informatized education certificates or they could provide

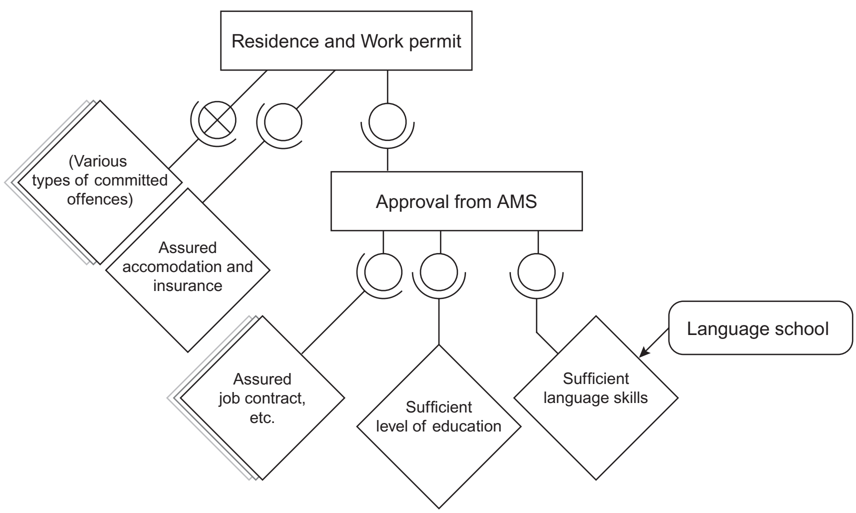

Fig. 14.2 Validity of residence and work permit as determined through constellation-based reasoning.

virtualized certificates of qualification. Such cyberspace-based assertions about an applicant's education could then be referenced by an Austrian nm-Gov registry that would hold education-related information. For qualifications received in systems that would not provide such linkable evidence, notary-like trusted service providers could act as translators from paper-based certificates to virtualized, linkable documents.

14.2 SCENARIO TWO: PARLIAMENTARY DECISION-MAKING

Modern parliamentary systems institutionalize democratic decision-making and regulate it through strict, formalized, procedures. The decision-making that follows these procedures is conducted by elected representatives of the political community. National assemblies, legislative councils, the Russian *Dumas*, Eastern *Majlis*, or Western *Parliaments*, etc., are the different names for the same concept of elected/hereditary/appointed representatives deciding on rules, investments, and other matters of the public domain. The process of making a decision by any such legislative assembly can be broadly divided into four distinct phases:

- first, the proposal is composed and presented to the assembly,
- next, the proposal is deliberated (often involving many instances),
- then, the assembly votes on the latest version of the proposal, and
- lastly, the proposal (if elected) is enacted and is put into action.

Fig. 14.3 depicts the legislative procedure in Slovenia, which has a bicameral legislature with a *parliament* (Državni zbor) as legislative body and a *state council* (Državni svet) as a second chamber, with a right to request a second round of deliberation on a proposal already accepted by the former. The parliament consists of a fixed number of 90 members, who in most cases decide by majority of the present assembly, whereby more than half of all members must be present for a decision to be valid.

A bill can be proposed by the government, any member of the parliament, or by at least 5000 voters. The process of deliberating and deciding on a proposal is defined as a multiphase procedure. First, the proposal must be sent to the president of the parliament and must contain an explanation for the cause of the proposed statute, its aims and goals, an estimate of the financial implications for the state budget if the proposal was to be enacted, a review of similar regulations in other legal systems, the compliance of the proposal with European Union law, and a discussion of other consequences the enacted law could imply. The president of the parliament initiates the legislative procedure by immediately distributing the received proposal among the members of the parliament.

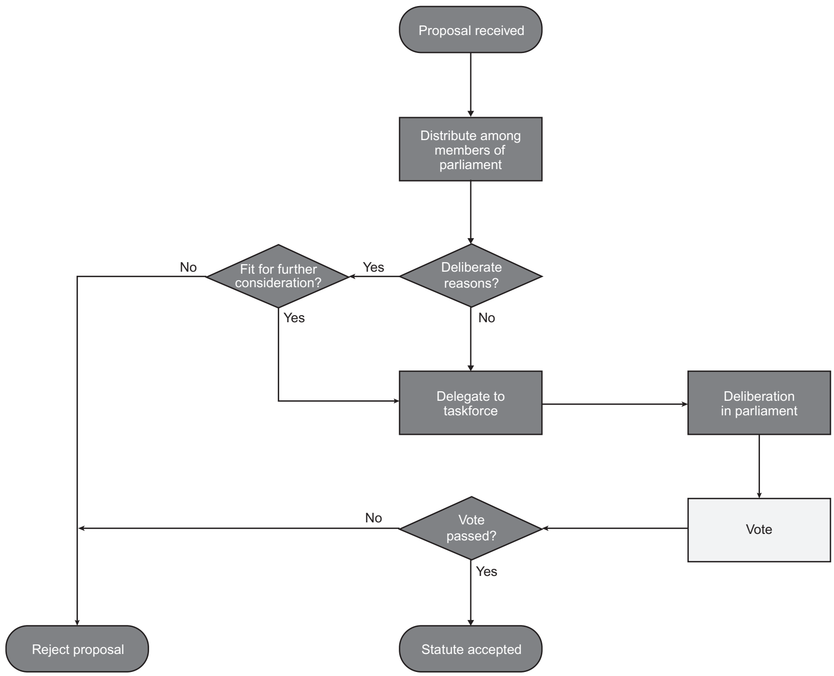

Fig. 14.3 Schema of legislative procedures in modern Slovenia.

Within 15 days, 10 or more members of the parliament can request a deliberation on the reasons for the proposal. If as a result of such deliberation the parliament finds that the proposal is not fit for further consideration, the proposal can be preliminarily rejected. If the proposal is to be considered further, it is delegated to a taskforce, to undergo deliberation such that it can be brought through amendments to a more robust stage before the taskforce presents the updated proposal to the parliament. The parliament then deliberates a second time on the updated proposal, where further changes can be made. Finally, a third round of deliberation takes place, after which a vote on the final version of the proposed statute is cast.

Could this process of the Slovenian parliament be handled by nm-Gov? The following are considerations on how such multiphase legislative procedures could be handled in nm-Gov, in two distinct ways. First, how it would be translated to remain virtually the same and, second, how it could be conducted by means of Liquid Democracy. For the sake of clarity, the second chamber of the Slovenian legislature shall be ignored, as well as any other possible exceptions provisioned in law, as such detail would merely introduce unnecessary complexity.

14.2.1 Existing Procedures Handled by nm-Gov

If the institutions, their roles, and functions, were to be kept in the transition to nm-Gov, then there would be four distinct agents who contribute to the enacted statute—the proposer, the parliament, the president of the latter, and the assistive taskforce.

First, the proposer would generate a proposal by writing it into the respective nm-Gov registry. The eligibility to write proposals into that registry would be given based on the qualification of the proposing agent—the agent would be either a member of the parliament or a representative of the government, or the proposal would have been signed by at least 5000 subjects with full citizen rights according to the voting registry. Once registered in the nm-Gov registry, the proposal would be available to the members of parliament (MPs) for deliberation.

If a minimum of 10 MPs indicated (within 15 days of submission) that they wish to deliberate on the reasons for the proposal, then the proposal would become blocked from being delegated to the taskforce. In such a case, a majority of MPs could either unblock the proposal (thus indicating that it is fit for further consideration) or reject it. The MPs would do so by voting on the fitness of the proposal.

If deemed fit for further consideration, the proposal would stay on hold until the taskforce would indicate that it is ready for the next stage. The members of this taskforce would have been appointed by the president of the parliament, who does so by enabling the membership in the appropriate nm-Gov registry. Once a majority of this taskforce would consider the content of the reworked proposal ripe for further action, they would write a collective assertion to the registry to indicate this.

Once labeled by the taskforce as ready, the president of the parliament would mark the proposal so as to denote that it had passed the deliberation by the taskforce. What follows would be a plenary deliberation phase during which the MPs discuss the finalized proposal. After plenary deliberation, the president would indicate that the proposal is mature for voting. Finally, the MPs would collectively label the statute either enacted or rejected—depending on whether the majority would take a "pro" or a "contra" stance.

Through the flow of changes in the status of the proposal, the proposal (as updated by the taskforce) would finally be enacted. However, unlike in present-day procedure which is governed by officials, the role of the agents taking part in this flow would focus on writing information to nm-Gov registries in order to change the readiness of the proposal, whereby their actions would be governed by the CBR locks of the nm-Gov registries. The transactions thus change from *push* to *pull*, i.e., the agents do not *push* documents to each other, but rather *pull* the status of the proposal and change it once the circumstances permit it. This implies the need for the periodic reading of corresponding registries in order to notify the agents on any changes, such as the appearance of a new proposal and the changes in its status.

The enactment of an accepted statute would also require a *pull*, rather than a *push*—any kind of *push* would require mediation which is undesired in nm-Gov. Accordingly, by a *pull* action, the statute would be enacted and thus change into law. In principle, anybody in whose interest it is to enact the accepted statute could conduct such *pull*—e.g., any MP or the proposer of the statute themselves. Today the enactment of a statute is limited to its publication in the official journal or similar media; in nm-Gov, however, an enactment of a new regulation would imply the immediate change of law. Complex constraints such as a certain required minimum time between the approval of a proposal and its enactment might be constructed in the form of CBR locks to prevent hasty action.

How, then, would the MPs deliberate on the proposal in nm-Gov? As nm-Gov does not deal with deliberation, but merely with the governance of eligibilities, it does not impose any constraints on how human beings exchange their opinions. Thus, if so desired, the *Parliament/Duma/Majlis* may remain as a place or institution where members and the public present their opinions in formal or informal ways, behind the lectern or in the lobbies, according to strict rules or traditional customs, or any other way that pleases the expectations of the society. The same liberty applies to other aspects of the procedure which leads to the enactment or rejection of a proposal, such as the flow of information about a new proposal and its change in status. People will continue to interact with each other offline, and accordingly, nothing is changed in the way they arrive at their decisions in an nm-Gov-enabled system.

What about secret voting? Again, here, nm-Gov does not set any constraints—thus, although CBR would require the identity of a voter to verify that the subject is a member of the eligible body, the identity does not need to be stored with the vote preference. This would be analogous to checking the identity of a voter entering the polling station.

14.2.2 Transformation to Liquid-Democratic Decision-Making

The basic principle of LD is that individuals can delegate their eligibilities to others in collective decision-making, but may temporarily repossess them to express their own decision in specific cases. The individuals' share of power in a collective decision is thus a frequently changing variable, rather than a foreseeable and fixed constant.

In terms of membership in a community that makes a collective decision, LD has no specific constraints. Accordingly, LD could be applied at several levels in the here discussed case of parliamentary decision-making, as follows:

- One option would be that only the (here, elected) members of the parliament take part in LD decision-making, whereby after they are elected they can delegate their voting power to their colleagues (e.g., to the presidents of their fractions), which might result in a significantly reduced number of powerful MPs and therefore transparently represent the power structures within the parliament. This approach might make more sense in larger parliaments, where the sheer number of members make decision-making less clear.
- Another option would be to treat the entire community of voters in a society as members of the LD system. This option could make traditional political parties obsolete, as the delegated eligibilities would shape into a network of a few very powerful nodes, to which large numbers of individual subjects would transitively link.
- A further option would be to take a hybrid approach where voters might have an opt-out option from the LD system by voting for MPs. The latter would then represent the entire community of voters who cast their vote in the elections, either in equal shares (i.e., each MP would have one vote in 90) or proportionally in accordance with the number of votes received. The voters that would remain in the LD modus might still be able to delegate their votes to MPs, or contribute their own decisions.

In either case, the multiphase mode could be maintained or transformed at will into a full LD-style decision-making single-phase process. While in the multiphase mode every changed state in the process of making a decision would be collectively decided through the logic of LD, in the single-phase mode a proposal would be accepted as soon as the required majority is formed through LD. In order to prevent hasty decisions, constraints regarding the time required for forming a decision could be set on a higher legislative level (e.g., on the constitutional level)—a statute could be passed, for example, after 1 hour once there is a consensus from *all* members of the voting body, or after at least 1 week once a two-third absolute majority is given.

For storing the LD relations between subjects, a dedicated nm-Gov registry would be required, in which each subject is able to address the attribute denoting to whom the voting power was delegated (if at all). The proposal being voted on might contain a snapshot of the network of relations at the time of its enactment/rejection for the sake of accountability/documentation. The snapshot of the decision on a particular proposal would remain dynamic and modifiable until the point that a decision is made. Thus, each subject would be able to either actively change their preference at any time until the final decision, or remain passive. By doing nothing, the subject would either passively support another member, if they have delegated their power to somebody else, or otherwise simply abstain from the collective decision-making.

14.3 SCENARIO THREE: PUBLIC FUNDING

The most important aspect of the public apparatus is the existence of a system of public funding. Public hospitals, schools, firemen, the army, and the public television are systems whose infrastructure, employees, and equipment are paid for out of the public budget, as are the salaries and offices of judges, mayors, ministers, or prosecutors, to name but a few. These public institutions are funded out of the same budget as roads, bridges, railway tracks, telecommunication infrastructure, sewage systems, and so on. Sports, culture, youth projects, politics, social care, science, etc., are also often existentially reliant on the drip of the public budget. Each of these can be abstracted to being understood as a *project*. A project can then be, for example, a periodically reoccurring endeavor such as the annual school year, or a single-occurrence undertaking such as the construction of a bridge, a space mission, or an international sports event.

Nation-level programs such as a public schooling system or public health care are projects of a special kind. What makes them special is their continuity over many decades, their complexity, and their vast scale. Nevertheless, these types of programs are projects that rely on public funding, have management, and so on. To this end, they are just as much of a project as the construction of a new school building, the purchase of a new fire engine, or a diplomatic mission. What all these projects have in common is that at some point they were proposed to some organization with sufficient funds for their realization. The chosen organization would have discussed the proposal, approved it, and provided means for the realization of the project.

In bureaucratic decision-making, the distribution of financial means available (or planned to be available) is conducted in a trickle-down manner. In Slovenia, for example, municipalities are funded through the state budget, which is approved through a specific statute by the parliament. The funds made available to each municipality are then further divided by the municipality council, which provides funding for the municipality's bodies and programs, as well as providing funds for further distribution to cultural, sport, or youth organizations, either through direct transfers or through open calls. The recipients of such funds would then further divide their funding into concrete small-scale projects.

This kind of trickle-down transfer of public finances from the national budget to concrete projects implies that public capital goes through a multitude of hands, incurring significant transaction costs and thus a reduced effectiveness of the available assets. The anecdote of the finance minister of Frederick II of Prussia on inefficient revenue sharing as recounted in Section 1.3—the minister used a cube of ice passing many hands to illustrate the flow of public capital from the treasury to concrete projects—might often fit as a comparison to the reality of the modern *revenue chain*.

What an annual budget does, in essence, is that it allocates a share of the whole budget to an organization, which can then be consumed by this organization within the budget year. Much like the cascading transfer described above, the share is further divided among organizations on the next level of beneficiaries, and so on.

To handle this through nm-Gov, a set of policies would be composed such that the budget-receiving organization has permission to access the given sum of money. Each organization participating in this distribution of money would in turn be able to create their own policies that allow lower-level organizations to access a share of the parent organization's (the organization that provides the funds) part of the overall budget. Subdivisions could intuitively be expressed in the form of percentages to describe the shares of all organizations receiving funds from the same organization in relation to their parent organization. Such relative shares would make it easy to recursively calculate the final sum of money that would be available to a specific receiver of the budget.

This expression of a budget as percentages of the whole would change the paradigm of how a community's budget is distributed. Contemporary budget distribution relies on the transfer of money down a revenue chain, which means that each parent organization literally sends the money to their beneficiaries in the form of bank transactions. In nm-Gov, this process could remain the same, or perhaps be rethought. For example, a single nm-Gov repository could contain the global budget of a community, and a set of CBR rules could control the conditions under which a beneficiary can access common funds. Accordingly, beneficiaries would have access to certain informatized slices of this repository; informatized/virtualized receipts would document the financial transactions conducted by the beneficiaries.

On the surface, the method adopted by an nm-Gov-based solution would not differ significantly from contemporary e-Gov solutions. Section 3.4 discussed the case of the Slovenian MFERAC system, a national treasury management system, through which virtually all financial transactions of government agencies are transacted. There, MFERAC was brought up to demonstrate how unapproachable such e-Gov systems can become—the case presented was an unsuccessful freedom-of-information request that aimed to reveal the contents of the e-Gov system. While e-Gov artifacts act as black-box systems, whose controllers can easily turn them into sinecures, the solution offered by nm-Gov would bring the power to control a community's treasury back to a state where it can be controlled democratically.

14.4 SCENARIO FOUR: GOVERNMENT DATA

What about government transparency, open data, or sensitive government data that must be protected? Wouldn't the electronic registries of nm-Gov imply an über-transparent state with no care for data protection?

The principles that enable nm-Gov ensure that sensitive data remains protected by appropriate access control mechanisms despite the eligibilities that can be derived from it. CBR allows different rules to be applied when read access to the data is requested, rather than in the case of other operations. Thus, revealing personal data, such as a birth date, can be prevented in read requests, while this very same data still can be used behind the scenes in CBR as part of an access control policy.

Conversely, access to nonrestricted government data would be available to the public at any time, who could use it for inspection, statistics, and other advanced use. Freedom-of-information requests for government data, such as the ones described in Sections 1.3.3 and 3.4, where data of the salaries and activities of public officials were requested, would no longer require uncomfortable requests, lengthy procedures, and (legal) disputes, but rather would be a matter of standardized self-service *pulls* from the nm-Gov registries. Any interested subject would thus be able to get the desired information quickly and "un-bureaucratically" at any time, without the need to draw the attention of administrative agents to themselves.

State statistics, such as unemployment figures, domestic product, and education level, would become accessible to the public, rather than being the turf of some specific agency, as anybody at any time could fetch the correct figures based on predefined, standardizable queries. Eventually, cross-border interoperability of such statistics could be established, which would bear the potential to dramatically reduce the costs and improve the accuracy of global economic statistics and forecasts. The thus achieved improvement of accessibility to accurate data would enable individuals and organizations to discover novel uses for real-time data.

The open-government idea as discussed in Section 2.1.4, to make data collected by government agencies available for public use in machine-readable formats, would benefit from nm-Gov as a core enabler to lay the foundational infrastructure for the agencies' relevance and sustainability. The networks of nm-Gov registries would enable access to core data according to valid regulation, hence neither interpretation of rules and data, nor consolidation of the requested data would be required. Any kind of ambiguity that might surround the genuineness, completeness, and relevance of the government data made available would instantly become a matter of the past.

14.5 THE QUANTUM BUDGET AS A WAY OF LIQUID-DEMOCRATIC PUBLIC FUNDING

With the combined power of nm-Gov and Liquid Democracy, new approaches to public revenue and public spending can be realized. One such approach is the Quantum Budget (QB), an idea which will be explained below.

The informatized governance in nm-Gov could make it possible that taxes would not be transferred to a central authority but instead remain in the possession, though outside of the control, of taxpayers. The word *quantum* in QB stands for the amount/share of something—in this case, the community's budget—each member of the community has control over their own *quantum* of the overall budget. The sum of all quanta is the *virtual communal fund* (VCF)—*virtual* simply as it does not exist as a tangible "pot of money." Each subject would owe a certain amount of taxes to the community, feeding into the VCF. The amount of each subject's tax contribution to the VCF would be defined by the formula-based reasoning of the CBR mechanism. Accordingly, raising/lowering taxes would be done by changing the formula that would define one's contribution. Access to the VCF would be governed via the key:lock paradigm from CBR, and facilitated through the principle of transitive delegations from Liquid Democracy.

The informatized quanta that make up the VCF could be utilized to fund projects and programs in the community. As control could be exercised by means of Liquid Democracy, the QB would bring democracy to an unprecedented level and allow for creative new applications in terms of public funding and public revenue. Each member would remain in "control" over their quantum (their share) of the VCF. Exactly how much such quantum would amount to, or how exactly it would be defined, is not imposed by the QB, but is a matter of how the community would define it—again, by means of the CBR mechanism.

There are many different ways in which QB could be implemented in reality, reaching from extremely libertarian to extremely social. However, a discussion on which way is the most socially just exceeds the scope of this treatise. The following are examples that illustrate two different flavors: The first case is more libertarian, and each citizen has full control over the amount of their taxes owed to the community. The second case is more social, giving citizens control over an equal share of the VCF—the quantum of those who do not pay taxes is equal to the quantum of those who pay a lot.

14.5.1 Example: Renovating the Community Library

For the sake of illustration we come back to the community from our explanation of Liquid Democracy in Section 3.5.1—Ann, Bob, Carl, Dan, Eve, and Franck. Ann owes the community 100 BTC (Bitcoins) in taxes; Bob owes 200 BTC; Carl, Dan, and Eve owe nothing; and Franck owes 300 BTC. The VCF of this community thus has 600 BTC available—the sum of all owed contributions. Ann has delegated her power to Bob, Bob and Carl to Dan, and Dan to Eve; Franck has not delegated his power to anyone. Ann would like to renovate the community's library, which would cost 333 BTC. Accordingly, Ann would need to raise 333 BTC with the help of the other members of the community.

If each quantum would be equal to the amount of one's tax contribution to the VCF, then the control of the quanta would be as follows (Fig. 14.4): Even though Eve pays no taxes, she would control 300 BTC in total, since Dan delegated his trust to her, and with it Bob's quantum of 200 BTC and Ann's 100 BTC. Franck would remain in control of his 300 BTC.

To raise the needed 333 BTC, Ann could convince Eve and Franck to make 333 BTC available—each could give, for example, half of the required sum. If Eve declined to support Ann's cause, Ann could revoke her delegation to Bob and use her own 100 BTC and then convince Franck to support her project with the remaining 233 BTC.

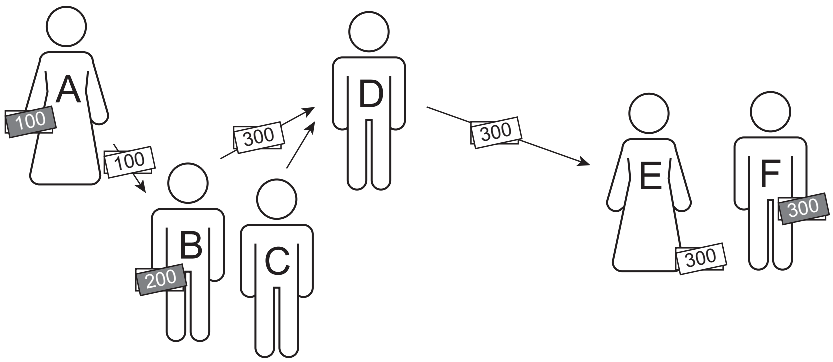

Fig. 14.4 Contribution-based quanta in the Virtual Communal Fund (VCF).

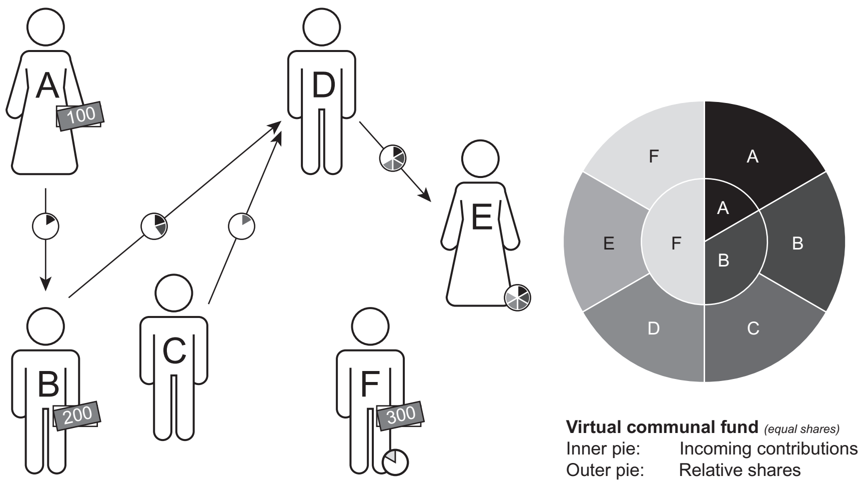

Fig. 14.5 ***Quantum Budget (QB) with equal shares.*** Independent of their contribution, each member of the community controls a quantum corresponding to an equal share of the VCF.

Alternatively, if each quantum corresponded to an equal share of the VCF, then each member of the community would have 1/6 of the VCF (100 BTC) at their disposal (Fig. 14.5). Given the LD delegations described above, Eve would control 5/6 of the VCF (500 BTC) and Franck his 1/6. For Ann to raise the needed 333 BTC, she could either convince Eve (controlling in total 5/6 of the VCF of 500 BTC) or Dan (controlling in total 400 BTC), or the other three each of whom control their own 100 BTC.

Whether or not Ann's quest to renovate the library would succeed is dependent on the endorsement of the other members of the community, as well as how much money their quanta amounted to. In the above example, Ann could either approach the strong nodes in the LD network, or take a grassroots approach to raising the required budget. Each of the approached nodes would contribute as much as they would consider proper, if anything at all.

The members could also exercise control over the budget from a different perspective—by expressing their support by means of percentages of their quanta. Say, Dan would like to strongly support Ann and would devote 85% of his quanta to the library project, Bob would disprove of the project and contribute nothing, Eve would contribute 20%, and Franck 50% of his quantum. Carl would remain a passive follower of Bob, and Ann would give 95% of her quantum to this project.

Table 14.1 illustrates how much funding Ann would raise in such a case. In the libertarian model, Ann would be able to raise only 245 of the needed 333 BTC. Even though Eve and Dan, who were initially the strongest nodes (Fig. 14.4), firmly supported Ann's cause, Bob's active opposition to the project has withdrawn 200 BTC from the network and accordingly thwarted Ann's plans. In the social model, however, funding was successfully secured.

In essence, the QB allows each member of the community to remain in control of their own quantum of the VCF. How exactly this control is exercised is a matter of how the community would decide—the QB concept does not prescribe any specific method. One option would be to exercise control in the form of dedicating percentages to projects/programs, as in the above example. Accordingly, each member would dedicate a part of their quantum to continuous programs (e.g., national defense, public schooling, and environmental protection) or ad hoc projects (e.g., renovation of the local library, fixing a street, and repairing the sewage system). Furthermore, each member could remain in control over their contribution to a particular project, and could even reduce or increase it during project execution—this way, members could, for example, liquid democratically cut funding for a running military mission.

14.5.2 Discussion

In a real-world instantiation of QB, there would be a myriad of projects such as Ann's that seek funding. Smaller such projects could be funded through action on the level of neighborhoods, cities, guilds, associations, and so on. A town's sports club could, for example, motivate their members to fund a new gym—today, they'd need to convince the town's government to do so. In order to fund more complex operations, such as a health-care system, organizations could bundle projects thematically into umbrella projects, and approach

Table 14.1 Funding for library project

		Libertarian model		Social model	
Name	**Contrib. (%)**	**Quantum worth**	**Contrib. to project**	**Quantum worth**	**Contrib. to project**
Ann	95	100	95	100	95
Bob	0	200	0	100	0
Carl	85	(→ Dan)	(→ Dan)	(→ Dan)	(→ Dan)
Dan		$0+0=0$	$0+0=0$	$100+100=200$	170
Eve	20	0	0	100	20
Franck	50	300	150	100	50
			Total: 245		Total: 335

individuals to steadily dedicate a fixed percentage of their quanta to them. How such organizations would be organized internally, and how they would distribute the funding received from the community, would be entirely up to them. They could organize themselves according to Weber's model for the sake of internal stability, or any other form of organization. Examples of such organizations are NGOs such as Greenpeace or the Red Cross, various types of foundations, Islamic waqfs (Jafar-Shaghaghi, 2013), the Catholic Church, political parties, armed forces, and municipalities. Even modern republics could be seen as such organizations who compete for their subjects' quanta.

This way, QB progresses the funding of the public apparatus to a deeply democratic level. Through Liquid Democracy (LD), self-organized groups of taxpayers could take on developing grassroots projects without the need for funds to be routed through an administrative framework.

Anybody could have a "good idea" and propose it to the community. The community would then need to find appropriate support for such a project and a formal request for funding of the project must be made. Here, the community could be of any type—it could be the nation as a whole, a representative body such as the parliament or municipal council, or an ad hoc community such as a neighborhood, the members of an association, and the tenants of a condominium—neither nm-Gov nor LD pose any constraints in this regard. Once the project plan is approved, the representative of the project would gain the *eligibility*/mandate to pay bills from the VCF, or further divide the thus gained share to be accessed by other eligible subjects. Furthermore, no transfer of funds would be required, and thus the use of finances, financial reporting, and full transparency of spending public means would be achieved through the same step of paying an invoice from the VCF.

This unprecedented level of democratic control over a community's agents and agencies would enable its members to fine-tune the actions of their public apparatus by controlling their funding of projects. Each member of the community could individually decide what share of their taxes is available to which agency, project, or program. Instead of actively setting their shares, individuals could also delegate this power to others by means of LD and thus remain passive followers of a broader interest network. Even if they delegated the dominion over their tax share to somebody else, each individual could still withdraw or change (temporarily or permanently) their delegation at any time and thus regain control over how their money is spent.

The described approach would enable the public to exercise advanced control over public spending and, if required, withdraw the mandate of an already funded project. Amendments that renegotiate the granted amount could also be conducted by liquid-democratic decision-making, and would thus present a way for the community to collectively control a project during its execution.

Combined with LD, nm-Gov would enable advanced forms of revenue sharing with a flexibility that is simply impossible to realize through current administrative networks due to the unfeasible transaction costs. Empowering taxpayers to exercise direct control over what happens in their community with their contributions would be a novelty in modern times, although not entirely novel in human history. Ancient Greek city-states knew *liturgy*, a system of public revenue without exaction, which stimulated wealthy citizens to cover the expenses of government and communal infrastructure on a voluntary basis (Adams, 2001, pp. 65–69).

It is not necessary to dig through dusty archives of history scholars for finding arguments in favor of such citizen self-organization—Tim O'Reilly reports of a recent self-organized road repair job in Hawaii, where business owners themselves raised $4,000,000 and repaired a local street in 8 days, as the alternative was to waste at least 2 years for the government to deliver (O'Reilly, 2010, pp. 26–27).

What about social benefits, pensions, child care benefits? At the end of the day, all of these are transactions from the communal budget, to which a subject is entitled given that certain criteria are met. As such, they can easily be handled by the CBR of nm-Gov. Receiving these payments in nm-Gov is not a *push* action from the government, as it is today, when the government transfers money to one's account each month, but rather a *pull* from the communal budget, which eligible subjects are themselves responsible to undertake. Social benefits then are nothing but one's eligibility to access the state budget up to a certain amount within a given period of time. It goes without saying that the contemporary *push* can be recreated easily in nm-Gov by periodic *pull* requests, which a technical system could conduct on behalf of the beneficiary.

REFERENCES

Adams, C., 2001. For Good and Evil: The Impact of Taxes on the Course of Civilization, second ed. Madison Books: Distributed by National Book Network, Lanham, MD.

Jafar-Shaghaghi, K., 2013. The Development of the Legal Parameters of the Waqf Institution in Contemporary Iran and Its Socioeconomic Impact (PhD thesis). University of St. Andrews, St. Andrews.

O'Reilly, T., 2010. Government as a platform. In: Lathrop, D., Ruma, L. (Eds.), Open Government—Collaboration, Transparency, and Participation in Practice. O'Reilly, Sebastopol, CA, pp. 11–39.

SUMMARY AND OUTLOOK

This book started by providing an overview of the rift between the culture of a well-established bureaucratic class that has provided public governance for generations and the new untapped possibilities for transformation of public governance brought about by cyberspace during the last quarter of the 20th century. The culture of providing governance by means of a public apparatus has been criticized for its well-known flaws due to human agency: fallibility, corruption, incompetence, slowness, and so on. To this end, anecdotal evidence has been presented to illustrate how predatory informal networks usurp resources that they ought to protect, how slow and arrogant officials protract seemingly trivial administrative proceedings, and how agencies inefficiently deal with requests for data, which could be dealt with in next to no time if only the underlying procedures had been appropriately technicized.

But how, then, can governance be "appropriately technicized?" Over the recent decades, there has been significant effort put into technicizing public governance in the form of computerization and digitalization of front- and back-end processes. Accordingly, a significant shift has already occurred from past methods of governing the public to structured and automated reasoning. While street-level bureaucracy used to be the main approach in delivering governance, the invention of computing and informatics brought a shift to screen-level bureaucracy in which decisions can be made remotely, based on evaluating structured forms. This was followed by a shift toward system-level bureaucracy in which massive back-end systems automatically make decisions based on data available to the system in a virtualized or informatized form. These advances were brought about by the digitalization of previously nontechnicized procedures and yielded massive systems that are beneficial for government agencies, which thus can provide their social functions faster and more efficiently.

However, just because something is good for government agencies does not mean that it is good for the governed citizens as well. The introduction of digitalization to public governance has yielded a system of government that is mightier and more frightening than ever before. The technical systems, which are used to govern society, are massive machines over which lawmakers have lost control. The increasing *digitalization* of governance is leading to a future that surprisingly closely resembles Orwell's *Big Brother*—that is, a state in which future generations will have lost all democratic control over the class that governs them. While political philosophers today label politics and public discourse as *simulations*, thus hinting at the powerlessness and pointlessness of the democratic institutions that have been fought for, from the view of technology, the transformation of societal power could be characterized as one leading to a neo-feudal era. In such a neo-feudal world order, the digitalized systems on which public governance crucially relies turn into "too-big-to-fail" sinecures of agencies, which are able to demand more and more resources to keep their systems alive. With no leverage to control such systems and their agencies by means of established democratic institutions, digitalized governance threatens to cause more harm in the long run, despite the good it has so far achieved.

What can be done to secure a future for democracy in the digital age? By looking at how systems of power come to be, we know that there are no specific rules that govern how governance evolves or the direction it takes. The evolution of systems of governance is enabled by opportunity and driven by the zealotry and ambitions of individuals and organizations, who grasp opportunities as they appear. Accordingly, a redemocratization of digitalized governance is an opportunity waiting to be seized, in order to transform our world into something better. Awareness of this is important, as it enables taking an out-of-the-box approach to rethink how future governance can be provided, without being constrained by contemporary circumstances.

1 INFORMATIZING GOVERNANCE

Modern public governance relies on a *fiat* system of law, in which individuals are given active roles in affairs of governance and given access to public resources in order to be able to realize their roles—policeman, mayor, judge, professor, etc., are typical roles. This same principle also applies to organizations—they assume roles and are endowed with public resources in order to fulfill their roles.

The question of how to redemocratize public governance thus boils down to two components: First, how can the public roles and resources be controlled? Second, how can the functionality of digitalized systems be controlled? What both questions have in common is the objective to establish control over data or structure. This in turn introduces a third question—that is, how can we control structured systems?

Advances in technology have yielded four generations of controlling structure by means of technology. The first was mechanization, where previously unstructured activities such as manufacturing were tamed and turned into well-structured processes. Based on this structure, power-based automation could increase efficiency, followed by the introduction of computerization and digitalization that enhanced the systems' capabilities and precision to entirely new levels. With the evolution of cyberspace, informatized systems of control appeared, able to control real-world systems from within cyberspace. What makes informatization so special is that informatized artifacts (data, files, code) can easily be shared and coproduced from within cyberspace. This inherent openness of informatized artifacts and their ability to be shared easily within cyberspace enable an unprecedented level of cocreation and coproduction that can be seized to redemocratize and evolve public governance beyond the status quo.

With the quest for redemocratizing governance moving to cyberspace, it becomes necessary to also move the entities and structures that make up governance into cyberspace—they must be informatized. Public resources, such as taxes, are almost perfectly informatized today—global credit transfers happen online and are routed through systems like SWIFTNet, the de facto global spine for any kind of financial transaction from micropayments by credit cards to multibillion Euro purchases of large corporations. While individuals in their capacity as human beings obviously cannot be informatized, they can still feasibly be virtualized. The virtualized individuals can then be associated with informatized entities in cyberspace, which denote their eligibilities to act in societal roles (e.g., judge, professor, policeman). These informatized roles in turn could then be democratically governed from within cyberspace.

Having answered how to informatize the objects of control (i.e., the roles and resources), the next challenge to focus on is how to informatize the mechanisms of control. A trivial question—one might think—all it takes is to develop algorithms that would provide that part? Alas, such thinking is seriously flawed. The crux of governing through algorithms is their limit to function in situations that are known in advance, while societal governance is a living organism that evolves over time in unpredictable ways. Hence, in order to design a system for informatizing governance that would sustain through future changes, algorithmic governance must be set aside.

To think of an approach to governance that would deliver without using algorithms, one has to understand the role of algorithms in systems of governance in the first place. Algorithms encapsulate a particular behavior, which then can be used to automate repetitive tasks or to automate a certain reasoning process. While automation of behavior might be required for some tasks of governmental agencies (e.g., sending tax assessment notices automatically to a large number of receivers), it is not required for situations of decision-making. While making decisions, such as whether or not one is eligible to unemployment benefits, can be nicely encoded in an algorithm, there are also other ways of arriving at such conclusions.

The approach that was chosen in this book is the concept of constellation-based reasoning (CBR), which is based on set theory and relies on formulas, which define subsets of data that satisfy particular conditions. To get an answer to the question whether or not Ann is eligible to unemployment benefits, the algorithmic approach would navigate through a decision tree to find the answer. CBR, on the other hand, would define a subset of individuals that have this right and check whether or not Ann belongs to that set. While the algorithmic approach offers superiority with regard to computing costs, it lacks extensibility—the algorithm is a black box, which must be changed each time a new requirement is added. On the other hand, while the set theory-based approach of CBR incurs seemingly unreasonable computing costs, it offers a level of flexibility that is of utmost value for democratic governance. More specifically, the formula-based definitions of subsets can infinitely be stacked on top of each other, thus enabling a cascading application of heterogeneous, context-conscious, regulations.

Such a way of governing eligibilities by means of stacking formula-based definitions of subsets on top of each other enables that these formulas exist as informatized entities in cyberspace, which can be coproduced, deliberated, and collectively enforced to act as the law governing the roles and resources of a governed space. What is more, the modification of existing CBR policies or the introduction of new ones can themselves be governed by means of already enacted CBR policies, thus creating a closed-loop informatized system of governance that can be democratically controlled entirely from within cyberspace. This, then, is the framework that can be used to informatize governance.

2 NONMEDIATED GOVERNANCE

Digitalized governance leads society to a road of serfdom plastered with sinecures in the form of too-big-to-fail governmental back-end systems. *Informatized* governance on the other hand has been designed such that it can be subjected to democratic control. Once informatized, governance can be conducted in a novel manner, namely, without the need for human intermediaries to determine things like the amount of one's unemployment benefits or giving mandates to political representatives.

Such nonmediated governance—*nm-Gov* for short—would open new avenues for the progress of civilization. It would change the core paradigm of governance from a serviced/mediated model in which officials issue documents to assert one's rights into a model in which one's rights are determined by querying an online information system. This would result in a network of rights—a digital *fabric*—that would hold massive amounts of data, with detailed descriptions of the (legally relevant) relations that make up the public apparatus. The availability of such data would enable the discovery of new approaches to analyze economies, boost research and development activities toward new general-purpose technologies, and fuel industry and business by enabling new types of services to be provided to allow easier interaction with the fabric of the nm-Gov data.

Not only would nm-Gov enable a radically new type of open government, but open government would also be an integral part of nm-Gov. Although data on which governance of the public apparatus would take place ("*government*" data, so to speak) would be in an inherently nonuser-friendly form, this would give opportunity to free-market software developers to engineer applications that would visualize, interpret, or mash-up the available data and thus enable user-friendly interaction.

3 LIVING NM-GOV

The nm-Gov core infrastructure would come as a bare infrastructure to store jurally relevant data and govern access to it based on advanced access control policies that replace written law. On top of that infrastructure, industry and private business would develop user-friendly applications. An example of such a consumer-facing application could be an app that would facilitate the purchase of goods such as real estate, cars, and company shares.

We might consider Ann selling her flat to Bob for the amount of 1000 bitcoins (BTC). Ann and Bob would draft the agreement, which would be a jointly signed request sent to the nm-Gov system. This agreement would encompass three interdependent requests: The first would lock the ownership over the property for a certain period of time and give only Bob the right to unlock it during this time under the condition that the agreed-upon amount of Bob's BTCs have been transferred into the ownership of Ann; the second request would entitle Ann to change Bob's ownership of the BTCs up to that amount to her own ownership; lastly, the appropriately marked transfer of ownership over the bitcoins would then entitle Bob to request change in ownership over the thus bought flat to his own identity.

Bob, however, would not physically transfer money to Ann via, for example, bank transfer or cash. Instead, Bob would make a share of his BTC credit available for Ann to change into her possession—the credits would be stored in the same nm-Gov registry—so, only data denoting a change of ownership would need to be written. Such credit-based transfer of informatized barter between debtor and creditor has been a common practice in banking and trade for decades (if not centuries) and has been thoroughly automated by modern electronic banking, e-payments, and credit transfer systems.

Transfer of real estate ownership in traditional *mediated* governance systems relies on the action of third-party agents, such as notaries, courts, and land registries, whose role is to assure integrity and validity of the purchase. In nm-Gov, however, integrity and validity would be assured by the technical infrastructure itself, thus making third-party agents redundant.

4 POWER TO THE PEOPLE

The possibilities brought about by informatized and nonmediated governance in terms of democratic control are endless. While action of public agencies in mediated governance is governed by complex and slow systems of checks and balances, which in turn are governed by written policies that have to be interpreted and reinterpreted on and on, public action in nm-Gov could be steered and controlled with an unprecedented level of precision.

More specifically, two interlinked concepts for democratic control of public action become possible. One is Liquid Democracy (LD) as a way of advanced collective decision-making able to supersede traditional party politics. The other is the Quantum Budget, where public funding is conducted by means of an LD-powered peer-to-peer system in which taxes are not collected into a central fund, but instead remain in the possession (though out of control) of the respective tax payers.

Thus, established democratic control over public resources can redemocratize public action. So, if you are unhappy with your country dropping bombs on innocent civilians, don't protest against the warmongers, simply cut their funding!

5 BEYOND THE LEGACY

While nm-Gov has the power to evolve civilization a step further, it does not impose progress nor prescribe it. Accordingly, even if nm-Gov infrastructure was to be installed in an existing society, it would not change existing functions and power relations of legacy institutions, unless so desired. But progressing society beyond the status quo is not the only way how nm-Gov could unleash its potentials.

The ability of nm-Gov to provide complex governance with practically zero administrative overheads and the promise to eradicate the potential for conflict caused by administrative wrongdoings could make it a promising tool for self-governance. This could serve future pioneering settlements in environments yet to be discovered, where the initial population is too scarce to maintain an apparatus of complex bureaucratic institutions. Experimental settlements in remote areas such as Mars or populations on spaceships that would have to travel for decades or even generations could thus be provided with a solution for advanced governance of access to common resources, which would be capable of scaling and transforming as the society evolves.

Another area of application would be emerging settlements developed to accommodate the large masses of economically motivated migrants who seek a better future in urban centers of developed nations. In this regard, economist Paul Romer has proposed the development of dedicated charter cities, which would offer the masses of migrants a new chance as guests of a developed nation. In the scope of such charter cities, nm-Gov could play an enabling role in fueling the economic growth while providing an unprecedented level of equality and new opportunity in governance. Such charter cities would thus have the possibility to turn into genuinely smart cities built from scratch, taking all paradigm-changing possibilities developed during the 20th and 21st century into account.

6 A NEW OPPORTUNITY

The idea presented in this book is the basis of a truly mammoth task. Bringing nm-Gov to life would require extensive further research, massive engineering efforts, the development of new hardware systems for processing and exchanging large amounts of data, testing and validating the thus developed new technologies, and so on. Building the *next democracy* would require the education of average citizens in how to interact with nm-Gov and cultivate a new collective state of mind on societal governance, politics, and so on. Once properly established, nm-Gov would become the new culture that would mature, evolve, and perpetuate itself. Generations raised in nm-Gov would find it strange that in a distant past people used to rely on rigid structures such as political parties and ministries.

Living nm-Gov would give rise to a new class of professional agents with the necessary technical skills to help average subjects in their interaction with the nm-Gov system. As such, it would create new types of jobs, reshuffle power relations in society, and provide the basis for a new world yet to be discovered. It would give rise to new approaches to fund public services and how to steer their delivery. New ideas on how to integrate emerging technology to create a smarter future would emerge, be validated, and integrated into the fabric of future societies.

There is much yet to research and discuss in order to bring nm-Gov to fruition. The thoughts and ideas presented in this book are no more than a humble approach to thinking up a future led by the desire to debureaucratize and redemocratize society. Accordingly, the book is not to be understood as a blueprint for how to make things right, but rather as a point of departure for further intellectual input on the matters at stake.

INDEX

Note: Page numbers followed by *f* indicate figures, *t* indicate tables and *np* indicate footnotes.

E

F

K

L

M

N

R

S

SMART
CITY GOVERNANCE
ALOIS PAULIN

- Explores the development of sustainable governance by examining how public domain governance can leverage the full potential of smart city technologies
- Provides insights on the technical side of the smart city governance
- Fuels discussions on how tomorrow's urban public institutions can contribute to a more inclusive and participatory society
- Provides a system architecture blueprint based on the insights and lessons learned

Empowerment and governance of people and resources are critical competent of what makes smart cities happen. Designing information systems capable of serving political and legal systems that absorb changes is essential.

Several books have been written to advice city governments on how to make their city "smart." This book, however, has different objectives. It follows the question of how smart city governance can be *informatized*—that is, how city governments, providers of communal services, and other agents that have official power in making a city a better place can be controlled and steered by means of information technology from within cyberspace.

This question is novel. Public governance has always been a matter of institutions controlling individuals or other institutions. But over the past couple of decades, circumstances have changed radically. Digital natives perceive cyberspace as an integral part of their reality. In this reality, new ways of conduct are possible, which has allowed civilization to evolve to a new level. In the last few decades we have experienced a revolutionary change in how communication, transportation, and navigation take place; how ordering and shipping of goods are conducted; how research is done; how information is conveyed; and so on. Informatizing the *governance* of cities and other communities is the next big opportunity to be seized to advance civilization to entirely new dimensions.

Alois Paulin is an assistant professor in the Faculty of Organisation Studies in Novo Mesto, Slovenia. He researches public-domain governance, sustainable government information systems, and democratic collaborative decision-making and is a coeditor of *Beyond Bureaucracy: Towards Sustainable Governance Informatisation* (Springer, 2017) and numerous journal articles published in *Advances in Intelligent and Soft Computing, Computers and Security, Journal of the Knowledge Economy, and Journal of Universal Computer Science.*

Political Science/Public Policy/City Planning and Urban Development

ISBN 978-0-12-816224-8

9 780128 162248

ELSEVIER

elsevier.com/books-and-journals