INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES

The Digital Era 3

Customs and Practices

Edited by
Jean-Pierre Chamoux

ISTE
WILEY

The Digital Era 3

Series Editor
Fabrice Papy

The Digital Era 3

Customs and Practices

Edited by

Jean-Pierre Chamoux

ISTE

WILEY

First published 2022 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

© ISTE Ltd 2022
The rights of Jean-Pierre Chamoux to be identified as the author of this work have been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s), contributor(s) or editor(s) and do not necessarily reflect the views of ISTE Group.

Library of Congress Control Number: 2022936006

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78630-192-5

Contents

Note to Reader

Being associated with computers and telecommunications, data and digital processing are omnipresent in today's society. Administrations, companies and even leisure activities produce, disseminate and manage data that represent human activity and their interactions. These data, which are the raw material of information industries, are the vital fluid of our society. This is why our era can rightly be called the "digital era".

Many experts were consulted in order to build the framework of this series of books on the digital era. The initial idea matured over 3 years. The outline, which was agreed upon in early 2016, includes three volumes. This collective work aims to describe and understand the technical, economic and social phenomena that result from the generalization of the Internet; the digital network that has been present everywhere since the end of the 20th century.

The first volume[1], on the issues of massive data, summarized the challenges presented by the enormous collections of data that have accompanied human activities for some time: demographic, biological, physical, geographical, political, industrial, economic and environmental data. These data feed columnists, inspire humans, guide their businesses and even their states. This first volume therefore illustrates the practical, technical and methodological advances that are associated with big data.

The second volume[2], on revisiting the economy, studied the reasons for and the way in which the digital world is transforming market exchanges, relations between

1 Chamoux, J.-P. (ed.). (2018). *The Digital Era 1: Big Data Stakes*. ISTE Ltd, London, and John Wiley & Sons, New York.

2 Chamoux, J.-P. (ed.). (2019). *The Digital Era 2: Political Economy Revisited*. ISTE Ltd, London, and John Wiley & Sons, New York.

people and their living conditions. How does the digital wave, which was described in the first volume, impact our lives? Based on the political economy since Adam Smith, is the wealth of nations shaken or transformed by these changes? How are the media, trade and inter-personal exchanges evolving? Why is wealth formed and how is it diffused and transmitted today?

This second volume emphasized that the new digital economy is not stabilized. Did it not take a good century for the political economy to adapt to the industrial society? Why would it not take as long for the political economy to integrate the data that is specific to the society of knowledge, which futurologists from the 1970s were already predicting[3]? Reflection is progressing and leading to disruptions, which the contributions in Volume 2 have carefully examined.

This third volume, devoted to mores and practices, concludes this series of works. It attempts to put into perspective some of the social issues that the digital era presents to our contemporaries, with particular intensity. Some of these questions were raised in the first two volumes; they are repeated here so that the readers can feed their own reflection and contribute, if need be, to the multiple public debates raised by the "issues of the new century"[4], which are anything but consensual!

This volume is based on experienced specialists from a wide range of backgrounds. The authors have written freely, as they should; they have inserted their contributions into the overall scheme that we have proposed to them. We owe them a great debt of gratitude. We would like to thank them sincerely for their scholarly contribution. As for the shortcomings or errors that could not be avoided, as usual, only the project manager is to be held accountable[5].

Jean-Pierre CHAMOUX
April 2022

3 Kahn, H. and Wiener, A. (1967). *The Year 2000, A Framework for Speculation on the Next 33 Years*. The Hudson Institute, Macmillan, New York.

4 Ellul, J. (1954). *La technique ou l'enjeu du siècle*. Armand Colin, Paris [*The Technological Society*, Knopf, New York, 1964].

5 The "editor's notes" in this book are those of the coordinator, Jean-Pierre Chamoux.

Foreword

Letter from America: The Great Transatlantic Divide

Let us not yield to a myth: even in the *digital era*, giving up all our privacy is not inevitable! With a little ambition and reflection, we could regain control over our identity and our *digital image*, provided we get out of the clutches of the so-called specialists and technocracy. To do so, we just have to make privacy popular again and open a public debate about it among informed and adult citizens.

First of all, let us stop blaming technology for a flaw that is not of its making: neither technical progress nor the generalization of the Internet should be blamed for the multiple indiscretions that disrupt us every day. Technology does not explain everything. If our intimacy is being disrupted, it is companies and very powerful administrations that are to blame: they are the ones who seize, keep and exploit personal data, which describe our person and our behaviors.

In America, contrary to in Europe, the legal system does not impose the protection of personal data according to a true "categorical imperative", similar to that expressed in the German and French laws of the 1970s[1].

This does not mean that American law is indifferent to privacy; nor does it mean that federal and state laws, and case law, neglect the privacy of individuals, the protection of their beliefs, their homes, their property and their reputations. The Fourth Amendment of the American Constitution, for example, safeguards the citizen against unreasonable search and seizure; case law has restricted the improper

1 Bundesdatenschutz Gezetz of January 27, 1977, and the French Data Protection Act of January 6, 1978.

dissemination of defamatory facts, and in several specific sectors, such as health care, banking, videotape rental, etc., personal data are regulated and at least as well protected in America as in Europe.

It is necessary to be well informed in order to know and identify these various protections, and to know how and why some personal information, under certain circumstances, is explicitly protected while other personal data can be collected, used and disseminated almost without limit. This legal system does not derive from a single general founding principle. Therefore, very large organizations can multiply the processing of personal data without the data subjects being able to oppose it; in truth, nobody knows, with certainty, what is recorded, by whom and why. In short, it is difficult and complicated to protect oneself against unwanted surveillance.

Reversing the current practice is, however, entirely feasible: one only has to look at the European Union to discover a world that is policed differently to ours in this respect. Faced with the same techniques that work in America, the options open to Europeans are different. We could therefore not only take inspiration from what is currently happening in Europe, but sometimes go further so that people can have real *positive rights* over the information that represents them.

The current institutional response boils down to two assertions: (1) that restricting the processing of personal information in private enterprise would inhibit the *free expression* of business[2], and (2) that limiting widespread state surveillance of the population, it is argued, could seriously threaten national security. As a result, the federal government can collect personal information on individuals at will, whenever national security requires it[3]. There is currently no "default" principle in the United States that defines what public and private bureaucracies can – or cannot – do with the personal data they hold. This is very different from the situation in Europe, which Wolfgang Kilian[4] summarizes as follows: "Unlike European law, the American system assumes that everything that is not prohibited is legal!" Those who

2 Editor's note: the great importance of constitutional texts in America is well known. Among the dozen or so amendments made to the American Constitution by the Bill of Rights (drafted in 1789 but ratified 2 years later, on December 15, 1791), the *first amendment* establishes rules that are much more liberal than those of other Western democracies: "Congress shall make no law abridging the freedom of speech or of the press".

3 Editor's note: in 2001, the Patriot Act abruptly expanded the powers of the executive branch, to the detriment of legal safeguards, for any case involving a presumption of "terrorism" (see Chapter 6).

4 Editor's note: distinguished professor at the Hannover Law School, W. Kilian is a respected expert in computer science and law; see our collective work with which he was associated, as well as J.B. Rule and others: Chamoux, J.-P. (1986). *L'appropriation de l'information*. LITEC, Paris, 99 sq.

deplore this situation would like to recover a true respect for privacy and intimacy, to restore rights and practices that would bring about true *ubiquitous* protection of privacy and intimacy, and would like that technology be put at the service of this right instead of undermining it, as is currently the case.

The first priority would perhaps be to formulate the general principle of personal data protection. This could be based on what is known in Europe as a "legal basis", which would involve an explicit contract with the subject concerned (e.g. the contract between the customer and their bank or the customer and their supplier); one could also imagine that any collection of personal data would result from a mandate entrusted by the subject to a large public or private organization, with which they are necessarily in close contact (for taxes, civil status, children's school, etc.); and finally, consider that the subject concerned must express their consent before being recorded and registered (to participate in a survey or a consumer panel, for example)[5].

It would also be desirable for the general public to be familiar with personal information systems, and for each citizen or consumer to be able to find out – for example on an Internet site – what is recorded about them; as well as for each individual to have the *right to access* personal information concerning them, a right that has long been accepted in France, Germany and Sweden in particular. Abuse or concealment should then be clearly reprehensible.

Lastly, we could grant *two positive rights to the data subject*: (1) the right to explicitly say whether they accept that their personal data can be used by a third party; and (2) that they then benefit from a counterpart that can be monetized, a sort of "property right", which could lead to the possible commercial use of the data in question[6]. In the absence of such an agreement, the *default* rule should be to respect the privacy of the subject and therefore *such exploitation should be prohibited*.

None of the assumptions above is really new[7]. Several of them are more or less in effect in Europe. Others, already mentioned in the literature, have never been

5 Editor's note: if such a framework existed, any broker of personal data would have to convince people to join this activity (which would probably lead to them being paid).

6 Editor's note: on this subject, see Chapters 1 (geo-tracking), 2 (algorithmic risk), 7 (right to be forgotten) and 8 (data protection and consumerism).

7 Editor's note: dedicated to the memory of George Orwell, the book published by J.B. Rule *et al*. 40 years ago already laid the foundations for a sociopolitical analysis of privacy in the modern world. He announced, in his introduction and essence, that people were beginning to understand that certain fiscal or social data could be diverted from their purpose; and the indignation raised by such practices was the real object of his book: J.B. Rule, D. McAdam, L. Stearns and D. Uglow (1980). *The Politics of Privacy*. Mentor Books, New York, 5–6.

applied in America until now. Our guiding principle is quite simple: we would like to illustrate how *privacy can be seriously respected in America* in a concrete manner, without condemning those who do not care about it and who therefore willingly hand over their privacy, which is their personal business.

Many forces would undoubtedly oppose such an evolution. However, the cause has not yet been lost, especially since it does not require going to war against technology; this has never been our intention, quite the contrary[8]!

James B. RULE
April 2022

8 The book by J.B. Rule, *Taking Privacy Seriously. How to Create the Rights we Need While we Still Have Something to Protect* (due to be published in 2023), extends and clarifies the work the author has been doing for many years on this vast subject.

Introduction

Mores and Practices

I cannot introduce this last volume of our collaborative work without expressing my deep gratitude to all those who have contributed to it: to the contributors who have abnegated to the rules imposed by an encyclopedic and didactic ambition; to the professionals that we have approached, listened to and disturbed in order to pass on their experience and their understanding of the techniques and knowledge of the digital era; to the learned colleagues of various origins and disciplines, because of whom we have recognized, over the years and through our readings, the new and the old, the absolute and the likely and, sometimes, the true and the false.

All of them have had the patience and courtesy to help us decipher the transboundary complexity of the world in which we have been immersed for half a century, whose key data, that are sometimes invisible, can be deceptive. The project, which began more than 5 years ago, could never be completed; we are putting an end to it without regret, being well-aware of the vanity involved in this choice, which I hope we will be forgiven for! The aphorism of Frédéric Bastiat, one of the free spirits of the 19th century who is better known in the United States than in France, just as Alexis de Tocqueville was for a long time, suggests this final thought[1]: for the digital world as for the economy, never forget that "behind what we see, what we don't see also allows us to understand the real world".

Textbook cases...

In Chapter 1, **Paul Salaün**, a lawyer specialized in the new techniques of communication and the Internet, marks out the issues put forward by the multiple

---

Introduction written by Jean-Pierre CHAMOUX.

1 Bastiat, F. (2005). *Ce qu'on voit et ce qu'on ne voit pas*. Romillat, Paris.

connected objects which invade our daily life and looks at the corresponding expertise. He focuses particularly on human freedoms and the autonomy of the person, on our relationship with automata and on the philosophical options that guide the proselytes of transhumanism. The author is very attentive to the evolution of European law, which is the subject of part of this chapter, but he strives to inscribe the practice in the existing law, without excluding that it is sometimes useful to imagine new rules when it is proven that the disruption really requires it. *Civil liability* has well-integrated technological issues[2]. Firmly based on case law, his diagnosis is cautious: he emphasizes that civil case law has taken up many challenges over the last two centuries, both in Romano-Germanic law and in Anglo-American liability law. After dealing with major innovations (automobiles, elevators, electricity as well as the errors of a misleading object like the connected assistant Alexa), we should trust that law in the future. For a long time, he notes, robots were confined to executable, programmable and repetitive tasks: driving a machine tool, driving a mining machine, mowing a lawn. However, the digital disruption, he underlines, means that we should consider that certain tasks, conditioned by the circumstances and by the environment of the robot, really put forward new questions to its owner (and to its operator): it is the very emblematic case of the driving of an autonomous vehicle within automobile traffic, which allows him to ask such questions. The relative autonomy of the machine does not yet reach the mythical capacities attributed to cyborgs (cybernetic organisms) by science fiction authors, mainly American. These *beings*, which are essentially imaginary, haunt the daydreams of those who tend to confuse reality with fiction: the similarities between the robot and the thinking being are purely formal, and risk inducing a fantasy drift, which the legal practitioner must absolutely beware of.

Chapter 2 is a real textbook case: it is based on the work of a research team of Germanic tradition, from which European law has drawn a great deal of inspiration, both for the competition law that has governed economic behavior for more than half a century, and for the carefully calculated *balance* between economic agents, some of whom are presumed to be weak, namely the consumers, while others, the merchants, are presumed to be strong and organized. The three authors, **Florian Saürwein**, **Natascha Just** and **Michael Lätzer**, address an important aspect of the digital economy: the pressure exerted by discreet but powerful algorithmic procedures on Internet users in general, and particularly on consumers. Fed by a considerable mass of nominative data collected by e-commerce machines, search engines or cell phones, the algorithms of digital platforms suggest consumption, services or entertainment that they presume the recipients are fond of (personalized and targeted advertising, in particular). This chapter describes and compares various

2 Article 1382 (new art. 1240) of the French Civil Code: “any act of man which causes damage to another person obliges the person by whose fault it occurred to repair it”, a tradition similar to that of damage in America or Great Britain (Tort law).

forms of supervision (regulatory or contractual) that could neutralize the fear expressed by a part of the population, who feel helpless in the face of algorithmic surveillance. Extending German ordo-liberalism, the school of regulation has often suggested, over a century, that public regulation should frame the behavior of public services, networks, agricultural markets, energy, raw materials, etc. Protecting the consumer against the solicitation of traders is one of its classic concerns. The same is true for tenants against landlords and industrial workers against their employers, etc. The authors propose a range of remedies to counter the mistrust expressed by a part of the public toward algorithms: should the initiative of advertisers be self-limiting in order to improve the relationship between the producer and its customers? Should we develop professional ethics? Should we limit the intrusion of automata in the life of the consumer and the Internet user (to prevent forced sales, for example)? The introduction of stringent regulations in certain areas leading to the "policing of algorithms" could be conceived at the European Community level by extending the existing provisions on the *protection of personal data*[3]. The authors conclude, however, with caution: algorithmic applications are recent; European society as a whole has not yet really estimated the real risks to our freedoms, or the positive repercussions of these methods, especially in terms of public health and the prevention of major catastrophic or cataclysmic risks[4]. This chapter therefore suggests measured recommendations: everything should be done, the researchers suggest, to better describe and understand the combination of various modes of action, partly political and partly behavioral. Keeping algorithms under careful surveillance seems to be the minimum objective for them, until practice – and case law – proposes a credible action to guarantee the future of our free will.

As illustrated in Chapters 7 and 8 of Volume 1, health and care are activities whose organization and perspective are challenged by digital tools. The processing of medical data concerns patients, practitioners and biotechnologies alike. Chapter 3 illustrates the effect of information technologies on the order of things and on professional practices. Taking advantage of the prospective method, **Sylvaine Mercuri Chapuis** and **Thomas Gauthier**, both academics, worked together at the Geneva School of Management (HEG). They designed a study that consisted of scenarios to illustrate the evolution of the Swiss public health system under the

3 Complementary provisions to those studied in Chapter 7 (the right to be forgotten) and Chapter 8 (data processing and freedom).

4 Many algorithmic methods can monitor outbreaks of an epidemic. Individuals are tracked by locating their cell phones; subject to inventory, this alerts the carrier to the presence of infected people. These successive contacts spot the spread of the virus; however, this method can lead to *social control*, the emblematic example of which is the facial recognition practiced by large Chinese cities (testimony by Sébastien Faletti for *Le Point*, November 27, 2018). Several countries (such as Taiwan and South Korea) have implemented such applications, but with uneven success (*Le Temps*, August 29, 2020).

pressure of digital technologies. As in all modern countries, public health in the French-speaking part of Switzerland (five counties of unequal size: Geneva, Fribourg, Neuchâtel, Vaud and Valais) is overwhelmed by a growing demand for care. Neither the ageing demography of these counties nor the contributory capacity of the working population seems to be able to guarantee a sustainable response to this explosive demand. This prospective analysis involved more than 60 collaborators, most of them students at the HEG in Geneva. It has a double documentary interest: first, because it concerns one of the European populations best provided with infrastructure, income and logistical support; and second, because it underlines that no "gamble" can promise the Swiss people – neither in the French-speaking counties nor in the German or Italian-speaking counties – a way out of the deadlock that condemns the rich countries of the world (mainly the United States, Western Europe and Japan) to let the cost of health care drift unchecked. The survey suggests that new technologies can indeed support the health care effort and contribute to limiting the budgetary drift that affects the care, therapy and hospitals of a modern country. As in most of Europe, care and expenditures are not balanced in Switzerland; the race to diagnose is costly and the price of targeted therapies is increasing faster than the population's ability to pay. The Swiss health system reveals rigidities and limitations that are confirmed by its vulnerability to unforeseen events[5]. Despite its very high standard of living and the excellence of its pharmaceutical and instrumental industries[6], this health system depends on international exchanges in several essential aspects. Like many other countries, Switzerland is highly integrated into international trade and finance; this strength could be a problem if the borders were less open to trade than they have been in the last 30 years. Switzerland, however, has a shortage of health care workers (doctors, nurses, pharmacists, therapists, service personnel, etc.); built around a complex mechanism of insurance, mutual funds and cooperatives, health care and medicine are looking for the Holy Grail of financial equilibrium without achieving it. In the scenarios summarized in this chapter, there is no evidence that the digitalization of diagnosis, treatment and services will stabilize the demand for care, the price of dependency, the price of hospital management and the price of medical procedures. Connected devices could, of course, transfer some of the tasks to patients that professionals would originally perform, tasks that machines are already able to take over (simple analyses or diagnoses, for example). However, the technology is not free for either professionals or patients; in addition, places would have to be equipped for this. Unfortunately, the prospective approach reaches its limits when the established system (which is based on a tight flow of services and care) comes

5 The Covid-19 pandemic, which was not included in the hypotheses of this research, confirms this diagnosis.

6 Industries concentrated around the capital city of "Swiss pharma", the German-speaking counties of Basel.

up against unforeseen circumstances: the next prospective analysis of Swiss health could therefore (perhaps?) be devoted to crisis management!

Lastly, Chapter 4 addresses a broad, fundamentally international and general topic; that of the *digital disruption* of the *financial sector*, which includes banks, stock exchanges, insurance and non-bank intermediaries (pension funds and investment funds), as well as typically digital financial instruments, such as *foreign exchange markets*, *derivatives* and *cybercurrencies*, whose innovative but disruptive role for traditional finance was discussed in previous volumes[7]. The result of a long cooperation between the coordinator of the book and two contributors with different experiences, backgrounds and perspectives – **Gérard Dréan**, author of three chapters in the previous volumes, and the economist **Henri Lepage**, an informed and critical observer of the international financial system – this chapter attempts to identify the elements of convergence or fracture that digital technology is causing within the monetary institutions we have inherited from history. The contemporary economy is constantly reshaping this legacy through technologies that ensure the ubiquity, functioning and security of financial markets and money. In contrast, the monetary institutions themselves, such as the central banks, the World Bank, the International Monetary Fund and the treasuries of major modern countries, in their purely political aspect, have proven to be cautious. This chapter, written by several people, continues the developments devoted to cybercurrencies in the previous volumes: it recalls that the financial crisis that disrupted global finance from 2007 to 2009 provoked the birth of *bitcoin*, the first cybercurrency conceived without any political or social imperative. Despite strong criticism, there has been an undeniable success of many electronic currency tokens. Money, credit and currency have not emerged unscathed from this crisis and from the disruption caused by bitcoin: rifts have disrupted the (apparently solid) whole of global finance. As for the monetary institutions, established 75 years ago, they were based on principles that contemporary society no longer accepts: the convertibility of the dollar into gold was abandoned in 1971; the economic and political balance of the planet is no longer the same as it was after the global conflagration of 1939–1945. The financial crises that have shaken the world since 1950 have raised questions that remain unresolved to this day, although they have been hotly debated at times. It is therefore an opportune time to bring out the subtle (sometimes visionary) analyses of past authors, whose essays are too often forgotten in this day and age!

... and political issues

Four issues are addressed and put into perspective with particular detail in the following chapters. Chapter 5, conceived by **Paul Salaün** already mentioned, takes

7 See Chapters 5 and 6 of Volume 1 and Chapter 7 of Volume 2.

stock of a catch-all expression that has been agitating the professional microcosm and regulators for more than 30 years. It addresses a seminal question: can the management of Internet networks – which are the direct heirs of telephone infrastructures – submit to a simple and general standard, inspired by the history that considered telecommunications to be a universal infrastructure and required it, without bias or privilege, to transmit thought, knowledge and interpersonal exchanges for the benefit of human beings as a whole? This chapter will show how out of step this universal claim is with the realities of the 21st century, and how reductive such an ambition can be. Network neutrality is a polysemous issue that the literature has been addressing for years without guiding the reader, even an informed one, or establishing their judgment. Paul Salaün's *variations* introduce some order into this subject, which is too often debated in a disorderly fashion. The spectacular growth of the firms that animate the world Net and their financial weight[8] lead a part of the doctrine to think that it would be necessary to supervise these behemoths that Internet users plebiscite. Inspired by a tradition of "universal service", we could, for example, impose constraints on network operators, similar to those of the old-fashioned telephone. However, the author dismantles several *fables* that go back to the time, long before the Internet, when communication networks had only a single use: since the 19th century, telephone wires only transmitted the voice. With the exception of North America, these lines were state-owned and operated by a public utility. Not very widespread outside the industrialized countries, the telephone provided uniform services, a requirement linked, in France, to the *neutrality* of the public service, which prohibited any differentiation between beneficiaries. Paul Salaün outlines the multiple connotations of an expression as a fuzzy *melting pot*! *Network neutrality is too polysemous to guide action*. In the end, the quarrels (political, doctrinal or judicial) that have pitted the multiple parties involved in the growth of the Internet against each other for 30 years leave a bitter taste. The often-Byzantine arguments put forward by the various parties to convince the public, the authorities or the courts, mainly in North America and Europe, can be summarized in a few words: some try to reformulate the *principle of a public service* extended to current networks, with the hope that the Internet will be inspired by a redistributive policy; others would like to confine the platforms and break up the largest ones (the GAFAs) to the benefit of dispersed agents; others, lastly, would like to rehabilitate the institutions that regulate communication country by country, authorities that have been called into question because the globalization of the Internet makes them ineffective.

8 These are, of course, the five most prominent stocks on the U.S. stock market, Google (or rather Alphabet), Apple, Facebook, Amazon and (to a lesser extent today) Microsoft, companies with impressive market valuations. Since the beginning of 2020, in the midst of the health crisis, the importance of these companies, driven by the demand for remote services, has grown even more.

The subject that **Pierre Schweitzer** addresses is very different to the previous one: Chapter 6 presents divisive questions, like all questions that concern *grand politics* as well as *shadow politics*, both dear to Machiavelli, in a deeply dialectical relationship. Between the utopia of "absolute transparency" (which would expose everyone to the more or less unhealthy curiosity of a stranger) and the opacity of regimes that cynically play with their peers or with their perverse inclinations, reason still hopes that a policed society is possible. The Internet has revealed, in various forms, the worst and the best in human beings and their social life. Well-researched, this chapter subtlety goes through the aberrations, scandals and practices that periodically agitate the network of networks since the *big names of this world* have been trying to use its performances to further their political ambitions. We discuss here upon a matter where reality is permanently rubbing shoulders with fiction, where real behaviors exceed what one can imagine; in short, it is a field where *Realpolitik* and warrior instinct meet! These pages have the great credit of leaving hardly any question in the shade and of underlining that the last 20 years have been marked by an unbridled use of information and communication technologies, all over the world, often to the detriment of our carefree and quiet life. The dramatic series of attacks that struck North America on September 2001 has permanently reversed political priorities. As in the days of the *Cold War*, the surveillance of people, their actions and their assets has once again become a priority to the detriment of the freedom to act, to enjoy one's property, to come and go and to cross borders without hindrance. The tolerances that we considered as rights have been called into question. Distrust has replaced the optimism that had characterized American society for so long. It has yielded to the State's reasoning and put the technological power of the digital industries at the service of the tutelary and repressive power of the federal government, and its central administrations. Pierre Schweitzer has immersed himself in this subject, full of unspoken words; he describes the facts and circumstances, the remarkable events and the key figures of this period that provoked a *Copernican revolution* in political mores, a change of perspective from which we are not ready to emerge, since the attacks of September 11, 2001 have created a climate of suspicion that has permeated behavior. The author looks back at the characteristic facts of those pivotal years (from 2001 to 2012, roughly), at the role and inspiration of the "whistleblowers" who challenged the mighty America, and at the effect these events had on the rest of the world. He describes the abrupt shift in political priorities that characterized this period. Using the case of France, he shows that a nation that has been involved for centuries in a part of the world, where the pan-Islamic threat is very active, is multiplying coercive, sometimes liberticidal measures. Under the pretext of public order, exceptional jurisdictions and procedures that are antinomic to an equitable and serene rule of law are multiplying. It also underlines the interaction between the security inflection of our institutions and the inquisitorial tendency that now frames the human person and the citizen, their private life and their autonomy. This chapter echoes the themes of the following chapters, but in a different form.

Chapter 7 resumes and summarizes the study on the *right to be untraceable* conducted by **Michel José Reymond**, a lawyer at the University of Geneva, then in residency at the Berkman-Klein Center for Internet & Society at Harvard University because of a grant from the Swiss National Science Foundation. Well circumscribed, this study is of general interest: the ruling handed down by the European Court of Justice on May 13, 2014 (known as "Google Spain"), settled an issue that conditions the exercise of two fundamental rights for the *digital individual*, both defined by pre-existing texts in Europe – the subject's *right of access* to nominative records kept by a third party and his/her *right to have contentious records rectified*, two issues that neither national laws nor the European Regulation on Personal Data (GDPR 2016) had really framed. Michel José Reymond dismantles the facts and the argumentation of the parties in a dispute that is linked to the implementation of the regulation, even though it is subsequent to this case. A more recent ruling ("Google CNIL" of September 24, 2019) also emphasizes the relative *nature of data protection with respect to other principles* that the Court considers to be of a higher order, such as *free expression* and *access to information*. Reymond concludes that the *right to be digitally forgotten* and *dereferencing* by a search engine or an Internet platform are delicate concepts to implement, and that the Luxembourg Court has taken a shortcut by entrusting Google with the task of managing individual cases through a quasi-arbitration procedure that could be considered, if prolonged, as essentially discretionary.

Carefully prepared and documented by **Michel José Reymond**, Chapter 8 completes this second part of the book. Inspired by individualistic principles, the doctrine developed in Europe in the early 1970s was based on two principles: respect for the human person and their private life; and the hierarchy of standards that placed the individual and their autonomy at a higher level than any of their economic interests, deeming that considerateness to the human person exceeds their material interests, no matter how important. Priority was thus given to a personal right, of a higher essence than economic utility, an approach consistent with the mandate of the Council of Europe since its foundation in Strasbourg in 1949[9]. The laws enacted as early as 1973 in Sweden (then a country outside the European Community), in the United States (1974), Federal Republic of Germany (1976) and France (1978) were thus in harmony with Convention 108 of the Council of Europe (1981), but without any direct link with the prerogatives of the European Commission. The purpose of these founding texts was not to *protect data*, but to prevent nominative data from *putting a human being under the control of a machine* or a mechanical process that would limit his autonomy, his freedom to act or to express himself. Such rights have nothing to do with any *kind of ownership*, as has been implied by excessive language; granted to the person on file, they only

9 A principle which was only remotely related to the mainly economic and social purpose of the European communities.

empower the individual with a *right of access and inspection* of the data that concerns them by name, and authorize them to have the content rectified if it contains inaccuracies (*right of rectification*). The community approach is now following a completely different path: it aims to establish a *free circulation of data in Europe*, which is extended, subject to reciprocity, to third countries such as the United States. This European law brings the protection of personal data closer to the rights granted to the consumer, which is confirmed by the General Regulation for the Protection of Personal Data (GDPR) that came into effect in May 2018. After placing the personal data regime in its historical perspective, this chapter clarifies the scope of this regulation, which strengthens the role of the European Commission in organizing the international exchange and retention of the massive data collected by Internet platforms such as Google, Facebook and Amazon, on all Internet users. The effect of this European regulation is not negligible; several disputes have already highlighted this. One of them is cited in Chapter 7 ("Google LLC vs. CNIL", September 24, 2019). The dominant position of American platforms, which are highly prized by Europeans, raises delicate issues, simply because these major intermediaries have a very strong presence in Europe and most of their personal files are processed and stored elsewhere than in Europe, particularly in the United States, where data on foreigners is easily accessible to police or legal authorities[10].

Evolution or disruption?

Chapter 9, written by **Ejan Mackaay**, Honorary Dean of the Faculty of Law in Montreal, attempts to place the preceding themes in their societal perspective. Western democracies are indeed torn between two contradictory inclinations: guaranteeing their people the positive freedoms promised by their institutions and protecting these same people against the unexpected and against external threats that could destabilize these same institutions. Maintaining the balance between the nanny state and the liberal state is never easy: Tocqueville once posed this dilemma in the following terms: "The love of order is confused with the taste for tyrants; and the holy cult of liberty with the contempt for laws"[11]. How do we resolve this apparent

10 The Court of Justice of the European Union has answered a preliminary question on this subject (case C 311.18: Data Protection Commission/Facebook Ireland & Maximilien Schrems): any transfer of personal data to third countries must be subject to guarantees equivalent to those offered by European law (GDPR). This is currently not the case under U.S. law, so the export of personal data to the United States is restricted. For a commentary on this ruling, see: Bradford, A. (2020). Broken shield: Privacy vs. surveillance in Europe. European Council for Foreign Relations, July 30 [Online]. Available at: www.ecfr.eu/article/commentary_broken_shield_privacy_versus _surveillance_in_europe.

11 de Tocqueville, A. (1981). *De la démocratie en Amérique*, Volume 1. GF Flammarion Paris, 68 [*Democracy in America*, Penguin Classics].

dilemma? In this chapter, Mackaay compares the behavior of six major democracies that, when confronted with the dramatic events of recent decades, have reacted quite differently from one another.

PLANTIN Jean-Christophe
Participatory Mapping

VENTRE Daniel
Chinese Cybersecurity and Defense

2013

BERNIK Igor
Cybercrime and Cyberwarfare

CAPET Philippe, DELAVALLADE Thomas
Information Evaluation

LEBRATY Jean-Fabrice, LOBRE-LEBRATY Katia
Crowdsourcing: One Step Beyond

SALLABERRY Christian
Geographical Information Retrieval in Textual Corpora

2012

BUCHER Bénédicte, LE BER Florence
Innovative Software Development in GIS

GAUSSIER Eric, YVON François
Textual Information Access

STOCKINGER Peter
Audiovisual Archives: Digital Text and Discourse Analysis

VENTRE Daniel
Cyber Conflict

2011

BANOS Arnaud, THÉVENIN Thomas
Geographical Information and Urban Transport Systems

DAUPHINÉ André
Fractal Geography

LEMBERGER Pirmin, MOREL Mederic
Managing Complexity of Information Systems

STOCKINGER Peter
Introduction to Audiovisual Archives

STOCKINGER Peter
Digital Audiovisual Archives

VENTRE Daniel
Cyberwar and Information Warfare

2010

BONNET Pierre
Enterprise Data Governance

BRUNET Roger
Sustainable Geography

CARREGA Pierre
Geographical Information and Climatology

CAUVIN Colette, ESCOBAR Francisco, SERRADJ Aziz
Thematic Cartography – 3-volume series
Thematic Cartography and Transformations – Volume 1
Cartography and the Impact of the Quantitative Revolution – Volume 2
New Approaches in Thematic Cartography – Volume 3

LANGLOIS Patrice
Simulation of Complex Systems in GIS

MATHIS Philippe
Graphs and Networks – 2nd edition

THERIAULT Marius, DES ROSIERS François
Modeling Urban Dynamics