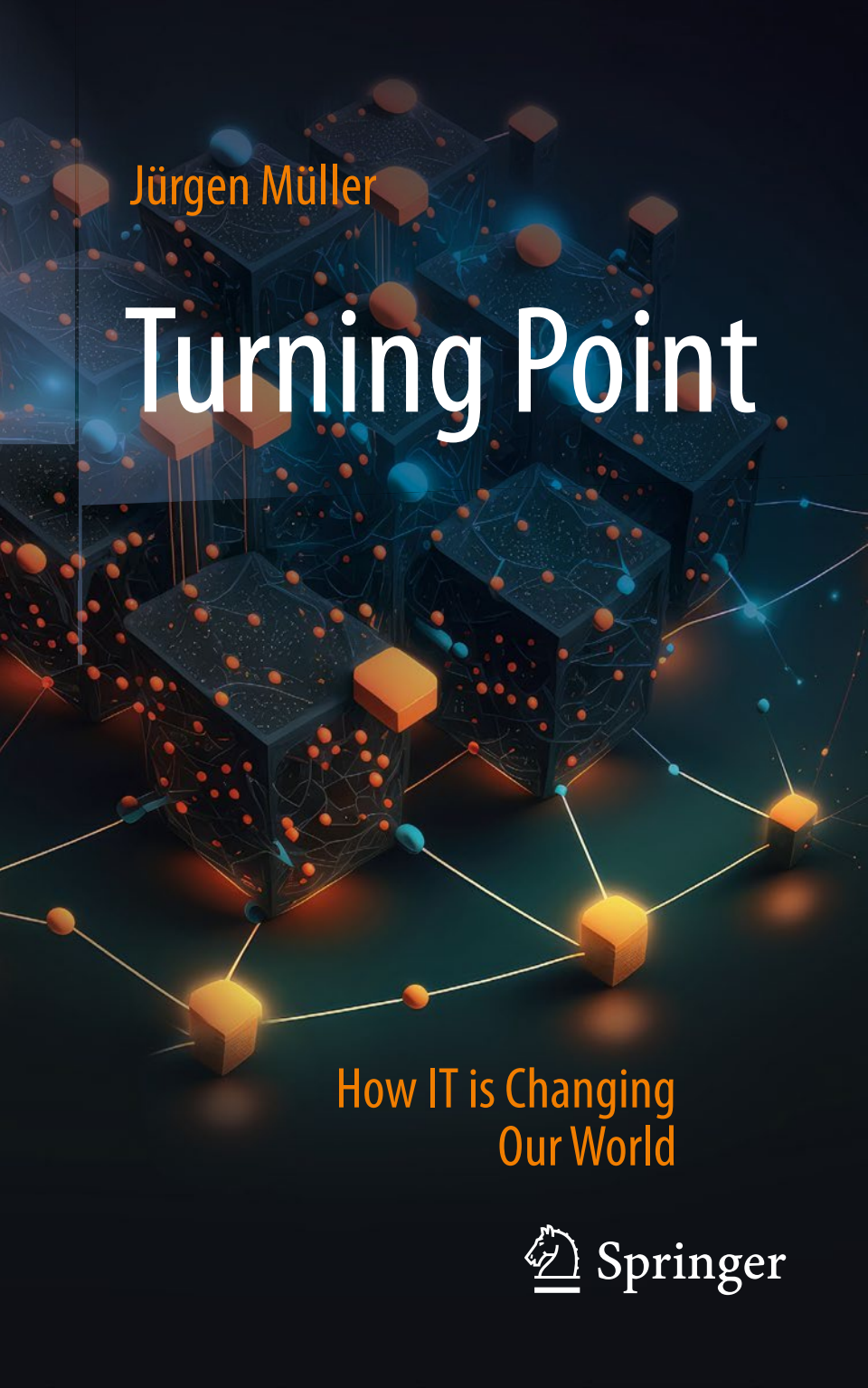
Jürgen Müller
Turning Point
How IT is Changing
Our World
Springer

Turning Point

Jürgen Müller

Turning Point

How IT is Changing Our World

Springer

Jürgen Müller
Düsseldorf, Germany

ISBN 978-3-658-46078-5 ISBN 978-3-658-46079-2 (eBook)
https://doi.org/10.1007/978-3-658-46079-2

This book is a translation of the original German edition "Zeitenwende" by Jürgen Müller, published by Springer Fachmedien Wiesbaden GmbH in 2023. The translation was done with the help of an artificial intelligence machine translation tool. A subsequent human revision was done primarily in terms of content, so that the book will read stylistically differently from a conventional translation. Springer Nature works continuously to further the development of tools for the production of books and on the related technologies to support the authors.

Planung/Lektorat: David Imgrund
This Springer imprint is published by the registered company Springer Fachmedien Wiesbaden GmbH, part of Springer Nature.
The registered company address is: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

If you think you are too small to move big things you never had a mosquito in your bed.

For Claudia, Fenja, and Thorin, as well as our four-legged family members, without whom this book would have been finished much faster.

Preface

The Eighth Day of Creation?

Does this headline serve to characterize the enormously rapid and profound changes that information technology (IT) is currently causing in all areas of our lives? Is the comparison to an eighth day of creation exaggerated? After reading the present book, hopefully, doubtful readers will have found an answer. We have become accustomed to distinguishing between the virtual world of computer networks and the "real," physical world. However, this distinction is not a faithful representation of reality. The cyber world and the real world have long since merged into a hybrid whole; the boundaries between our online and offline lives are fluid. This is the new reality, even if it presents itself to us as individuals to varying degrees. Social networks and the opinions expressed within them create "facts," they influence elections, determine politics, and reveal the white spots of state regulation and

jurisprudence. What happens on the net during the day appears in the news in the evening.

State hackers are engaged in a permanent cyber war, to such an extent that it is hardly possible to distinguish between war and peace. Is the crippling of the Colonial fuel pipeline in the USA in 2021 by Russian hackers or the infiltration—presumably by Israel and the USA—of the Stuxnet worm, which is only 500 kilobytes in size but had devastating effects on Iranian nuclear facilities in 2010, still peace or already war? Some countries have discovered "hacking" as a source of income and instruct their state-organized actors to extort foreign companies. They have become criminal organizations with a national flag and a seat in the UN. And when companies like Facebook or X (formerly Twitter) allow their users to call for violence against an aggressor on their networks, are they already parties to the war or not yet? Information technology is a master at blurring boundaries.

Some things have so far shown a remarkable persistence. Since their invention, we have been driving our cars with combustion engines, and we are still used to driving them ourselves. We pay our bills with state-guaranteed money in euros, dollars, or yuan and use a bank for this purpose. In our factories and offices, human labor is still a significant factor. But how long will we hold on to these habits? The very rapid, exponential networking of our world, the miniaturization of computers in the form of smartphones or sensors, and the increasing use of artificial intelligence are quietly but extremely effectively challenging them. IT is a stealthy force. Each of us is familiar with the first moon landing on July 20, 1969. Few will know the birth year of the internet. The moon landing has practically no perceptible significance for our everyday lives, yet it is still covered in history lessons. The internet has massively influenced our daily lives over the past 30 years, but it is hardly

mentioned there, if at all. Stealthy processes are less noticed than major events, regardless of their actual significance. We perceive the encroachment of IT into all domains of social life, economy, and politics as normal and only marginally notice the turning point associated with it. We are no longer even surprised that the processors in our cell phones contain transistors so small that millions of them could fit on the period at the end of this sentence. Even crime today is largely different from what it was before the IT era. Social life, economic progress, and politics are now closely linked to the development of IT.

Companies must reinvent their business models because IT enables and forces new forms of value creation, new sales, marketing, and logistics channels are emerging, and new production and development methods promise more efficiency and competitive advantages. Artificial intelligence is transforming entire industries, the way our children learn, and how medical professionals heal. It creates a precursor of "mind" in learning machines, and we are only at the beginning of this development. Traditional industry boundaries are increasingly dissolving, creating competitive situations that did not exist before. Those who were only active in the IT market yesterday are now also involved in the music business, offering financial services, and building smart home devices. Apple Music, Alibaba's Alipay, and Google Nest are just a few examples of this. The established giants within the affected economic sectors are facing competition from outside and are thus under pressure. Cross-industry business models are emerging, based on the power of digital technology. Those who fail to recognize this cross-sectional nature of IT or simply do not have the know-how and resources to utilize it are at a disadvantage. Those who can't keep up will be left behind. In the digital world, it is not the big fish that eat the small, but the fast that eat the slow.

State regulatory efforts lag behind an explosively mutating technology and new business models. Improvement is not in sight, although some states—like in the EU—are joining forces with others to intervene efficiently and across borders. However, they repeatedly hit their limits because the agreed measures are all too often meager compromises resulting from differing interests. Internet companies have the power, the money, and the influence to endure this cat-and-mouse game and secure the best locations. It is no longer a compelling requirement to be physically present where they want to do business. The reach of data centers is by definition global. National solo efforts prove to be the wrong path. "Tech nationalism" and isolation only work temporarily and conditionally; in the long run, they exclude from progress. This is especially true for economically small and medium-sized countries, but ultimately also for the giants. The restriction of conventional sovereignty associated with international cooperation is both a burden and an opportunity.

IT has changed the globe, has made it into a "global village," although this term from the 1960s hardly does justice to the current development of individuals, economy, politics, and society. We live in a new world. If one were to attempt to agree on a worldwide standard for a modern era, one could with some justification speak of "before the Internet" and "since the Internet." Such is the immense influence of technological development on all areas of our lives. Has the dawn of the eighth day of creation already begun? And what is yet to come?

Nothing is without history, and much can be explained by it. Therefore, this book also discusses the history of modern IT and the development of the technology underlying it in a way that is easy to understand. How did it come about, what drove it, who were the key players, who created the Internet, why do the United States dominate,

and why does Europe play only a minor role in this crucial field? However, it deals much more with other fundamental questions of IT. These include, for example: How and why and with what impacts does it change the economy and geopolitics? What role does it play in the new East-West power struggle? What goals do hackers pursue, who are these people, and who controls them? Another focus is on the influence of technological development on our social life, our work, and our thinking and actions. IT creates new forms of security needs, it exacerbates and clarifies the differences between authoritarian and democratic regimes. Where will this journey go?

In order to answer such and other big questions, I will draw on practical and real case examples that are partially based on my own experiences. Everyday topics that readers may have been interested in for a long time will also be explained, almost in passing. Examples of this are: What exactly is a digital business model, is there really such a thing as security in IT, what happens when you google, what do Artificial Intelligence and Big Data mean, what exactly is behind the multifaceted term of the Cloud?

When I entered the IT field as a career changer in May 1990, it was not a particularly good time for the industry. I remember exactly how I drove through Cupertino, Mountain View, Sunnyvale, and other places in Silicon Valley, where nothing suggested a gold rush atmosphere. In the front yards of numerous elegant houses stood a desolate sign: FOR SALE. Apple was limping, Windows had not yet established itself, Microsoft and Apple were arguing over the rights to the still quite young graphical user interface. A hint of the 1980s was blowing through the country, companies with long-forgotten names today—like Atari and Commodore—were still active in the market.

When I moved from Düsseldorf to San Francisco with my wife almost ten years later, the world was already a different place. The industry had once again shown how cyclical it operates. The internet had taken off, Google was in a steep ascent two years after its founding, and the Dot-com bubble was growing ever larger in the overheated industry. At that time, it was almost frowned upon for young companies to make profits. Instead, they endeavored to burn through money at a high rate based on a questionable economy. An end to the speculation and gambling did not seem in sight, even though it did come soon after. The index of the technology stock exchange NASDAQ had risen by 400% between 1995 and March 2000, when it reached its peak. At that time, I was looking for salespeople for my employer Sybase. Numerous career starters applied and demanded obscenely high salaries and many stock options on top of that. To most of them—not all—I said that although I did not know how I would manage without them, I would still like to try. The gap between the apparent competence and the demanded salary was just too large for me.

This book resembles a lesson on the changes that information technology has brought about in recent decades. For my research, I only occasionally visited a library and did not request any printed magazines or articles. My research was conducted almost entirely digitally; all important information was within reach of a mouse and keyboard. It was supplemented by online meetings with people whose thoughts and advice I consider valuable. What a contrast to the time of my studies in history and political science! Back then, I spent weeks and months in archives and libraries, ordered books through interlibrary loan, stood in line at one of the few university copiers, and then collected index cards with content and literature references in a wooden box.

"Non-digital," on the other hand, were the personal experiences from my jobs, the observations, and lessons from the last 35 years of my career during the creation of the book. It was the time I spent in different roles, companies, countries, and continents in IT. They are the actual foundation of this book; most of the questions, ideas, evaluations, and conclusions are based on them. Somehow, I find that reassuring. Personal encounters with other people are ultimately irreplaceable. Nor is the fun and sometimes the frustration that resulted from it. Only digital and theoretical and without extensive practical experience, this book would have become entirely different or perhaps not even come into existence.

The book is aimed at a broad audience and is for everyone who is aware of the fact that IT increasingly and more massively influences society, the economy, and politics, and that they themselves are personally affected. They generally only have a "felt" knowledge but feel the need for understandable and sustainable explanations. Most of us experience this process of change as a daily, almost inconspicuous sequence of small steps. This makes the realization of the big picture, the assembling of individual observations into a pattern and overall picture, difficult. This applies not only to people outside but also to many within the IT industry. Questions, as treated here, have significant professional relevance in everyday life for only a few actors even there.

The goal of the book is to convey this large picture with its bright and dark sides in a way that is easily understandable. I will try to highlight selected major lines, create awareness of the tremendous upheavals we are experiencing, explain developments, and in this way provide orientation and, above all, a piece of maturity in an increasingly technologized society. And something else is important

to me: I want to correct the prevailing, fear-oriented, and negatively colored discussion about changes brought by IT—as can be easily seen in the example of artificial intelligence—and to highlight not only its risks but also its opportunities.

It is good to give chance some space in life. I myself ended up in IT by chance; actually, an academic career in the humanities at a university was planned. I have not regretted the step into IT for a single second. Reinventing myself has done me good; when one door closes, another opens. Being able to work in a very dynamic industry, where you have to consider every morning in the shower why what was successful until yesterday no longer works today and needs to be reinvented, has always been a lot of fun for me. The IT industry rarely forgives mistakes; it is fascinating, intense, fast-paced, surprisingly often more art than science, and has enormous consequences for our lives. It falls in love with solutions, not problems. It knows that it is better to be 80 percent right today and implement these ideas with full force than to wait until a 100 percent solution is found. The motto of the hacker group Anonymous sums it up with immortal conciseness: "We are legion. We do not forgive. We do not forget. Expect us." Where else could it be more exciting? I look forward to constructive suggestions and criticism on my blog "zeitenwende-it.com".

Jürgen Müller

Contents

1

Beyond Technology. Our New Life with IT

"I have a device in my pocket that allows me to access all the information known to humanity. I use it to look at pictures of cats and argue with strangers."[1] This quote from 2019 comes from a user of Reddit.com, a social media platform that is especially popular in the USA. Computer technology has become so small and portable that it seamlessly integrates into all aspects of our lives in the form of smartwatches, smartphones, or tablets. The miniaturization of computers drives their usage. If we only had desktop computers available, we would certainly spend significantly less time on these devices. Perhaps our activities would also be significantly less trivial than described in the quote. Trivialization is apparently, among other remarkable phenomena, a variant of our behavior on the internet.

In a survey in the USA from February 2021, 46% of respondents stated that they spend an average of five to six hours daily on their smartphones, excluding work-related

J. Müller, *Turning Point*,
https://doi.org/10.1007/978-3-658-46079-2_1

use. Another 11% reported seven or more hours, and 22% said they spend an average of three to four hours daily on their phones. Only 5% claimed to use their smartphones for less than an hour per day. The remaining 16% were at one to two hours.[2] Assuming that our average waking time is around 17 hours,[3] smartphone consumption plays a significant role for large segments of the population—it dictates the daily routine. Of course, there are also apps on the internet that facilitate such number games and can simultaneously help us control our smartphone consumption. Examples include AppDetox, OffTime, or FlipD. They say nothing about the consequences of this form of constant strain, but they are obvious nonetheless. When parents or children spend their time on smartphones, personal interaction, through which social behavior is conveyed and shaped, suffers. This shaping, especially in children, should not be delegated to strangers on the internet. The internet gives us access to the world at any time and from almost any place. It is often forgotten that it also gives the world access to us. Not everyone who roams the internet has the best intentions. The wise Master Yoda from the Star Wars series aptly described it when he revealed himself as a harbinger of cyberpsychology: "When you look at the Dark Side, careful you must be. For the Dark Side looks back."

Digital Psychograms

Cyberpsychology is a young branch of knowledge that deals with the effects of digital interaction on human behavior. It refers not only to, but especially to, the internet. Evolution has not conditioned us for the use of technology, but for personal interaction with each other. "Post-sociality," the replacement of personal interaction

with communication technology, is not on nature's development plan. Therefore, many of our instincts do not function at the computer; our behavior is often not the same as in so-called real life. Our still very young millennium has brought humanity high-frequency crises of global magnitude in its first good 20 years. They line up like pearls on a string: the terrorist attacks on the World Trade Center and the Pentagon in 2001, the subsequent war in Afghanistan, the invasion of Iraq under false pretenses, which permanently and negatively changed the balance of power in the Middle East for the West. In 2008, a global financial crisis began, triggered by a real estate bubble in America. It was different in that it did not only affect stock owners but also the "ordinary citizen" who had to fear for their savings. In 2011, the civil war in Syria began as a result of the Arab Spring, which brought Europe the exacerbation of its migration problem. A similar problem later emerged in the United States, where people fleeing poverty and violence in Central and South America knocked on the door. This was accompanied by the debt crisis in Europe, virulent since 2009, which could have brought the end of the Eurozone and lasted until the middle of the decade. The list can be extended indefinitely, with the preliminary endpoints being the COVID-19 pandemic and Russia's invasion of Ukraine. All of this has deeply embedded itself in the collective consciousness. A significant reason for this is that these crises have an omnipresence beyond traditional TV and print media, primarily caused by the internet and its access via smartphones. They are the subject of more or less qualified comments on the Twitters (now X), Telegrams, and Facebooks of this world. Every change is communicated in real-time; there is always a fire somewhere, and we are under constant bombardment. The result is VUCA, "Volatility, Uncertainty, Complexity, and Ambiguity." Uncertainty rises, the

longing for stability, for simple explanations, for certainty. The internet is the outlet for the resulting discontent and the place where one can seek belonging and "friends."

In her readable book on the subject of "digital behavior," Mary Aiken has described a number of interesting phenomena that can be observed in our online lives.[4] She collectively refers to these as cyber effects, of which I would like to address the most essential ones, namely disinhibition, behavior reinforcement, syndication, and cyber migration.

Many of us have already experienced online disinhibition in a professional or private context. There are simply too many people who react in emails, chats, or on social networks in an exaggerated manner that they would never do in direct personal contact. Therefore, I made it my maxim many years ago to respond to such "electronic" outbursts of others—back then mostly via email—consciously delayed (or often not at all). Also for self-protection, because computer networks are young, but their memory lasts long. When such reactions culminate in hate speech, defamation, or threats of violence on the web, the fun definitely stops. There are numerous prominent examples of this, one being the case of Renate Künast. Here, a german politician was attributed with completely fabricated quotes, accompanied by obscene insults and rude threats. In a trial that went through several instances, the Federal Constitutional Court ultimately decided that Facebook must disclose the data of the authors so that they can be prosecuted. This must serve as a lesson to potential offenders. Like at any other crime scene, they also leave their electronic "fingerprints" on the net. It is naive to believe that one can evade detection with the means available to ordinary mortals. Cybernaivety could thus be seen as a new behavioral category. Anonymity is a myth that many users still believe in. It

makes transgressions as easy as their uncomplicated logistics. Anyone who has to write, print, envelope, and mail a scathing letter with the correct address is more likely to refrain from letting their bitter feelings run free. The effort is a deterrent. The computer and its keyboard take that away from us.

Closely linked to the easily made transgressions on the computer is a behavioral reinforcement that experts call online amplification. An interesting example of this is cyberchondria. This refers to anxiety disorders related to health that are generated or intensified by internet research. We don't feel well, the heart skips a beat, the stomach twinges. In a self-experiment, I entered the search term "stomach pain" and Dr. Google responded with diagnoses like "gastritis," "it could also be the heart," "stomach ulcer," "salmonella," "pancreatitis," until I finally ended up with stomach cancer and various self-help groups after intensifying the search. Suddenly, one feels like they have a serious illness without any medical findings. An everyday discomfort that could have been eliminated with a cup of tea takes on life-threatening dimensions, and uncertainty spreads. The phenomenon is well known to health insurance companies, as they have to bear the economic consequences of online hypochondria. Of course, it is no coincidence that website operators design their tagging in such a way that the number of visitors to their websites increases. The more dramatic, the better for the click rate. This is also reflected in the results of search queries.[5]

Harmless in itself, online syndication can grow into a serious danger when like-minded people with questionable views come together in groups on the net and confirm each other's opinions. Technology makes this immensely easier. Someone who is a follower of absurd conspiracy theories living in a sparsely populated rural area has little chance of meeting someone who thinks similarly. This

problem does not exist on the net. People who are on the same wavelength are easy to find in cyberspace. Suddenly, one is no longer isolated and receives applause for their opinion instead of negative criticism from their immediate environment. The conclusion many draw from this is: I am right after all. The next step is arranging a "demo" over the internet, thus getting to know each other personally. The feeling of being right is joined by the feeling of belonging to a community that knows more and is smarter than the mainstream—one belongs to a kind of elite that grows closer together through attacks from outside. Pegida, the most well-known german example of this, started as a Facebook group. This form of group formation can, in extreme cases, lead to strong radicalization, as a study by the think tank Rand Corporation based on concrete cases shows.[6] Where radicals previously had to go through the effort of physical recruitment with limited reach, they now use the internet as a political platform with a scattergun effect. Self-radicalization of individuals is a desired side effect.

Whether one can also speak of such desirability in the case of cyber-migration must remain an open question. Cyber-migration describes the adoption of behavior from the net into our offline lives, with the term being used in various ways, e.g., also for the migration of visitors between social networks. Given the significant amount of time we spend online, the idea of such adoptions is close at hand. The communities we join in social media, the opinions we encounter, the new "friends" we chat with, leave their marks on our thinking and actions. A kind of second socialization takes place unnoticed, influencing our physical world. The younger we are, the more pronounced this effect is. Personal experiences show that the attention span of my friends and acquaintances is getting shorter and shorter. Listening seems to be more difficult when the

partner does not communicate in "chat format." In email correspondence with colleagues, it can be seen from their responses that longer texts are not read properly; feedback leaves much to be desired after just five lines. Information is more likely to be consumed than thought through, responses must be spontaneous and quick, and are therefore sometimes deficient.

Not every person is equally susceptible to cyber effects. This is also why there is no reason for pessimism. People with a corresponding predisposition are more likely to be affected, while others handle it more critically and can derive great benefits from the internet. The internet is a mirror of society and is unlikely to lead to a world of behaviorally conspicuous people. What applies online is what also applies in our offline lives. Michael Seto, a Canadian forensic psychologist, once described the internet as "the greatest unregulated social experiment of all time"[7]. The internet is widely seen as an instrument and platform of freedom, and rightly so. It facilitates the expression of opinions, provides a forum for the voiceless, organizes democratic protests, is a reflection of diversity, and thus the bane of autocrats and dictators. They are therefore constantly striving to limit access to the web for their population.[8] The internet spreads the knowledge of humanity around the world in an instant and allows everyone to participate. It accelerates science and research, and allows us to connect with each other from almost any location.

Even the questionable aspects described have their positive sides, aside from disinhibition. Successful fundraising campaigns on the internet, whether for children with cancer, war refugees, or animal protection, represent a form of behavioral reinforcement and syndication. A very creative and interesting example of this is an event involving Airbnb, a leading broker of vacation rentals and rooms.[9]

In March 2022, Sarah Brown from Salt Lake City booked a room through Airbnb with Ekaterina Martiusheva in Kyiv to support people in Ukraine during wartime. She never intended to use it but checked in anyway. Airbnb pays the hosts 24 hours after the guest has checked in. Ekaterina received the money promptly, and in a phone call with National Public Radio (NPR), a kind of American version of Deutschlandfunk, she explained how much this donation meant to her. Spread via Facebook, Sarah Brown started a wave. Within two days, over 61,000 overnight stays in Ukraine worth over two million dollars were booked from around the world. When Airbnb noticed the event, the company waived the fees for all hosts and guests.

Those who transfer empathy to the internet also show a form of cyber-migration, only in the opposite direction. But as with any form of freedom, we must also handle freedom on the web carefully. If it is abused, whether by ordinary criminals, child molesters, extortionists, hate speakers, or political demagogues, boundaries must be drawn. The legislature has recognized this necessity, it is slowly making progress, but mostly acts reactively rather than preventively. It is like a journey into a new world because our legal system also needs to be adapted to these new opportunities and dangers. The universe of cyberspace is expanding much faster than the earthly realm of the legislature.

Life on the Platforms

In October 2021, there were 4.55 billion active social media users worldwide. In the second quarter of 2021, Facebook counted 2.89 billion active users per month, and Instagram one billion. Thus, 3.89 billion of all

visitors were attributed to Meta Platforms Inc., the company that owns these two market giants.[10] Other platforms have to settle for significantly less attention: Twitter (now X), Snapchat, Pinterest, LinkedIn. A look at WhatsApp and Facebook Messenger makes the dominance of the "Meta family" even clearer. Their messaging services Facebook Messenger and WhatsApp, which was acquired in February 2014 for $19 billion, handle more than 50% of the global messaging volume. Only TikTok and Google's YouTube play in a similar league with their video platforms. TikTok has even developed into a heavyweight among video platforms in a relatively short time.[11] It belongs to the Chinese company Byte Dance, which caused it a lot of trouble in the USA under the Trump administration and still does. Google's YouTube is still the top dog in this business with two billion monthly users. However, only about 30 million pay for its premium video and music service.[12] Measured against the approximately eight billion people on our planet, the penetration rate of these media is enormous. No one else can boast comparable reach. Their mere ubiquity gives them significant and determining weight in our daily lives. These platforms neither produce anything themselves nor do the vast majority of users count as their real customers. Having an account on Facebook or Snapchat alone does not make us one. Their business model is based on an almost ingenious idea: billions of users feed the platform daily, voluntarily, unsolicited, highly frequently, and for free with data. They form a kind of community of "freelancers" spread across the globe. A member of the Hamburg based Chaos Computer Club described it this way: "The saying always went at Facebook: The user is not the customer, he is actually the product."[13]

The core of the consideration is that users are allowed to create and communicate their own content via the

platform. The platforms then exploit the users' data, their comments, likes, messages, their uploaded content, their usage behavior, and much more by marketing them for advertising purposes of all kinds. These unpaid suppliers are ultimately the guarantors of their high profits. Data protection is written in small letters in this model. Those who value it more will quickly realize, when looking for Facebook-like alternatives, how great the compromises are that would have to be made in case of renunciation or change. "Similar" here means: messaging, sharing, likes, posting pictures, videos, and links. One of Facebook's larger competitors is Reddit, with over 50 million daily users.[14] Reddit's focus is in the USA; in Germany, despite partially localized content, there were only 3.9 million users. Overall, visitor numbers outside the United States are very small and fragmented,[15] which is why the attractiveness of local content or Reddit groups leaves much to be desired. The biggest compromise, therefore, lies in the reach of alternative platforms, as fewer users naturally also mean fewer opportunities for group formation and communication. With fewer participants, the economies of scale decrease. Almost all competitors, therefore, try to score with a combination of data protection, freedom of expression, transparency, and ad-free experience. They exploit Facebook's Achilles' heel.

Some position themselves as anti-Facebook. Minds, for example, says of itself: "Minds is a social open-source network that advocates for freedom on the internet. Speak freely, protect your privacy… and take control of your social media."[16] A whitepaper from Minds, which describes technology, content, business model, and the founders' motivation,[17] reads in its moral charge like Luther's theses against the Catholic Church, which he is said to have nailed to the portal of the Castle Church of Wittenberg in 1517. Minds uses a very modern approach

for data storage, dispensing with central storage and instead working decentrally with cryptographic blockchain technology.[18] Users pay for the provision of content via a network protocol that allows direct connection between them. This so-called Wire Protocol, therefore, does not need a central control and intermediary instance like Facebook, which allows it access to the data and its use. Payment can be made in the form of donations, ad hoc transfers, as well as subscriptions. The operators call this contribution economy, as opposed to platform economy, which Facebook stands for. Minds has—as of March 2022—around six million users.[19]

It goes without saying that such "uncensored" and uncurated social platforms also attract people whose access would have been blocked elsewhere due to their views and extreme statements. The small providers operate below the radar of state regulators, whose attention is focused on the larger ones. However, this automatically raises the question of how great the desire for data protection really is among the billions of visitors to mainstream platforms. Interestingly, it is not they who force such platforms to better data protection. They apparently do not care much about it; otherwise, they would simply switch to an alternative provider. The network effects associated with the size of Facebook, which I will discuss in more detail elsewhere, exert such a strong attraction that a switch—if desired at all—seems unattractive. The ambivalent role of the protective instance is therefore taken over by the state, which must navigate the narrow path between freedom and the protection of personal rights, but cannot always be entirely sure-footed in doing so.

Artificial Intelligence and Learning Machines

The terms Artificial Intelligence (AI), Machine Learning, Deep Learning, Algorithms, and Big Data encounter us in everyday life not only when it comes to the utilization of our data by platforms. Anyone using a navigation system in a car is guided by AI on an optimized route. On the packaging of my new electric toothbrush, I found the sentence: "Genius X with artificial intelligence has learned from the brushing behavior of thousands of people." This example shows how far AI has penetrated our lives. The aforementioned terms are often used with little distinction and mixed into an unspecific whole. This is understandable to a certain extent, as the boundaries between them can indeed be fluid. To better understand these terms, which we will encounter more frequently throughout the book, I would like to define them more precisely using concrete examples.

Artificial Intelligence is the umbrella term for a range of techniques that refer to the ability of computers to make intelligent decisions and thus emulate human intelligence. AI learns from the data it interprets and constantly improves its results in this way. The more data available, the more secure the interpretation and the stronger the learning progress and reliability of the results. Conventional software, on the other hand, follows a predefined, rigid set of rules dictated by the program. Because it—somewhat simplified—does not interpret data but merely processes it, it is not adaptive and therefore does not improve its results on its own. No matter how much data is available to it, the set of rules will always remain the same and determine the outcome. AI represents the transition from useful to smart computers. Automation

of processes is the main characteristic of useful computers. Smart is the main characteristic of computers with AI. They make intelligent decisions, are able to weigh alternatives against each other, and can independently generate meaningful content. The range of artificial intelligence spans from semi-autonomous to autonomous, meaning it can operate with varying degrees of human intervention. AI thus ventures into areas that were previously reserved for us humans. We will discuss a special variant, the so-called chatbots, in more detail elsewhere. They are used to simulate conversations with humans and have gained significant public interest. All of this generates fears among some contemporaries, resulting in AI often being seen more as a problem than an opportunity. The following example, which demonstrates its strong influence on our lives beyond practical use, represents its numerous applications.

Ping An Insurance from Shenzhen in southern China is one of the top three insurance companies in the world by market value.[20] It uses AI on a large scale for recruiting new employees, pursuing two goals: more efficient handling of the high recruitment volume and—more importantly—a better hit rate in selecting the right talents. Applicants must answer questions from intelligent machines during the recruitment process. Their answers are compared in terms of content, tone, word choice, and gestures with those of the company's most successful salespeople. Large amounts of data are available for this, collected from previous job interviews, among other sources. The feedback with the later performance of the hired candidates is used to constantly refine the system. At Ping An, they are firmly convinced that this system is better and more objective in selecting the right employees than the human interviews that follow later in the process.[21] Anyone who has ever been interviewed for a job and been