Hilde Nagell

# Digital revolution

## How to take your freedom and power back

Translated from Norwegian to English
by Adam King

With the kind support of the Stockholm office
of the Friedrich Ebert Stiftung (FES Nordic Countries)

Bibliographical information of the German National Library
The German National Library catalogues this publication in the
German National Bibliography; detailed bibliographic information
can be found on the internet at: *http://dnb.dnb.de*.

Original title: Digital revolusjon – hvordan ta makten og friheten tilbake
First published 2020 by Res Publica:
https://respublica.no/produkter/digitalrevolusjon/

ISBN 978-3-8012-3301-3


Verlag J. H. W. Dietz Nachf. GmbH
Dreizehnmorgenweg 24, D-53175 Bonn
Tel. + 49 (0) 228/18 48 770 / info@dietz-verlag.de

Cover design: Rohtext, Bonn
Typesetting: Kempken DTP-Service, Marburg
Printing and processing: Bookpress, Olsztyn


Printed in Poland 2025

Find us on the internet: *www.dietz-verlag.de*

# Contents

# Foreword to the English edition

In November 2022, the language model ChatGPT took the world by storm. Within a few days, it gained over 100 million users and became the fastest-growing app in history. Today, large language models are everywhere. In schools, at work, at home, in shops, or when accessing public services. The new language models made artificial intelligence concrete and part of daily life in an entirely new way, and it became a conversation topic for everyone. We have acquired tools that can write text, answer exam questions, generate images and video, or assist in coding advanced programs simply by means of a few sentences in natural language.

When a new technology exerts such great influence over how we write, learn, work, and seek information in so short a time, it raises fundamental questions about who defines knowledge, language, and truth. It is precisely such questions that this book seeks to help the reader pose sharply.

Artificial intelligence is far more than large language models, and for several decades it has already lain as an invisible backdrop in much of the digital services we use, both in the public and private sectors, often with great utility value.

The book you hold in your hand was written before ChatGPT. Digital power is less about apps and user experiences than about control over infrastructure: data centers, cloud services, cables, satellites, operating systems—and now also AI models. When a few actors both provide the storage of our data, the platforms we communicate on, and the models that "understand" and process our language, they possess a combination of power that is historically novel.

In the book, I describe how the world has moved further away from the ideal of an open, global network and more toward a fragmented and regulated "splinternet," shaped by geopolitical tensions, security policy, and industrial policy. These are developmental trends that have intensified in recent years.

With Russia's war of aggression in Ukraine, their internet has become even more controlled and delimited. Superpowers like the USA and China invest enormous sums in infrastructure, chips, data centers, and talent, competing to be first in the race. It concerns military applications, but also control over the economy, financial markets, communication, and knowledge production. Artificial intelligence is regarded as a key technology on par with nuclear power and oil in previous eras.

## Digital Infrastructure

At the same time, the political context surrounding these companies has changed. Donald Trump has again been elected president of the USA, and at his inauguration, the leaders of the largest technology companies were visibly present. This signals that the relationship between political and technological power has become even closer. Elon Musk was given responsibility for a period to "slim down" the public sector in the USA with a chainsaw, before the formal role disappeared, but the informal influence remains: for instance through control over satellite communication in war zones, ownership of global platforms.

When I wrote the book, I toyed with the working title "Musk and Power." Since then, it has only become clearer how much the digital infrastructure and a few companies are shaped by individual persons' choices and temperaments. Elon Musk's Starlink satellites are to provide broadband to large parts of the world. Since 2020, this project has unfolded on a full scale. Thousands of Starlink satellites now orbit the Earth, and the number is steadily increasing. and will make Starlink one of the dominant actors in satellite-based communication globally.

The question of who ultimately controls the digital infrastructure—a democratically elected government or a private actor—strikes right at the core of the book's theme of digital sovereignty.

## Free Flow of Information

The emergence of the internet is a story of a shared, collectively owned project built on open source, discussion pages, and information

sharing. Now it is increasingly subject to disinformation, conspiracy theories, and targeted influence campaigns. Moderation rules change, previous blocks are lifted, and algorithms are adjusted in ways that often give the most visibility to the most extreme and sensational content. When an AI model is directly connected to this stream, it becomes entirely central to ask: What does it amplify? Who controls the updates? And how does this affect what users perceive as "probably true"?

The trends I describe have not disappeared; rather, they have been reinforced by the AI boom. The same companies that dominated search, advertising, and social media are today central also in the development of the largest AI models. This means that the structures the book analyzes—surveillance economy, network monopolies, and the skewed distribution of power—now grip even deeper into our lives.

The book shows how a particular business model has emerged as dominant on the internet: the surveillance economy, where "free" services are financed by collecting, analyzing, and using our data to target ads, influence behavior, and build detailed profiles. We do not pay with money at the checkout, but with time, attention, and the intimacy of our lives.

Since 2020, this model has both become more visible and more challenged. Revelations about massive data collection, manipulative interfaces, and leaks of sensitive information have led to increasing unease. At the same time, more political environments, activists, and researchers have begun demanding a complete ban on surveillance-based marketing. They argue that the way we finance digital services is not technological fate, but a political and economic choice.

## Regulation

Today, we must place our trust in a few large private technology companies in our digital everyday lives—for search services, maps, social media, cloud storage, and software programs.

The EU has made major advances in regulating these companies. Three new laws have come into place. The Digital Services Act (DSA) concerns how platforms handle illegal content, advertising, transpar-

ency, and users' rights. It gives authorities better insight into how algorithms work, imposes requirements for risk assessments, and strengthens the ability to intervene when platforms fail to fulfill their obligations.

The Digital Markets Act (DMA) targets the largest platforms—the so-called "gatekeepers"—and seeks to prevent them from abusing their position to shut out competitors or force users into closed ecosystems. This may, for example, involve requirements for interoperability, prohibitions against favoring own services in search and app stores, and restrictions on how data from various services can be combined. The AI Act is the world's first comprehensive regulatory framework that classifies AI systems according to risk, sets requirements for documentation and transparency, and prohibits certain forms of particularly intrusive use, such as mass surveillance with facial recognition in public spaces.

These laws are important, but as the book argues: regulation alone does not provide control if ownership, infrastructure, and data management remain unchanged.

## Digital Sovereignty

Control means, among other things, being able to opt out of a platform without losing all access to services and networks, being able to move one's data between different providers, and having real, public alternatives to critical services. It also means building institutions—public, cooperative, civil society-based—that can develop and operate technology on premises other than maximal short-term profit.

For states, it means being able to decide over one's own digital infrastructure, data, and security without being entirely at the mercy of other countries' companies and authorities. For individuals, it means having real control over one's own data, digital identities, and everyday tools. And for communities—municipalities, trade unions, organizations—it concerns being able to organize, communicate, and collaborate on platforms they actually trust.

In practice, digital sovereignty is a balancing act. No country can "build everything itself," but some choices increase dependency more

than others. Placing public services, health data, and democratic debate in the hands of a few commercial clouds and platforms may be efficient in the short term, but costly in the long term—both economically and democratically. We must view digital infrastructure as part of society's foundation, on par with electricity, roads, and water.

## A Nordic Model for Digitalization and Data Sharing

The book argues for a Nordic model for digitalization and data sharing that combines a strong welfare state, high trust, and an active public sector with a willingness to treat data as a common good, within clear frameworks for privacy and rights.

Norway is largely a customer of others' solutions—we purchase cloud services, platforms, and AI models from American and increasingly Chinese-dominated companies. The question is whether we should merely attempt to regulate what happens, or also build our own alternatives: shared solutions, commons of data and models, and public or cooperative infrastructures that reduce dependency.

I hope the book can be read as a starting point for critical reflection on which actors and values actually govern digitalization and the development of artificial intelligence. Who wins and who loses? What alternatives still exist for us as a society and community to take back some of the power and control over the development? These questions have increased rather than diminished in importance.

Oslo, December 2025

# Introduction

As a child I would often draw on large sheets of paper with light blue and white lines and perforated edges. They came from the computers at the Norwegian Institute of Technology's Computing Centre in Trondheim, where my father worked. I remember the racket and whoosh of those huge machines and the way they heated up the whole room where they sat. Today, the world's smallest computer could fit inside a grain of rice.[1] Meanwhile, computing capacity has grown and grown: in 2019 the Norwegian University of Science and Technology (NTNU) acquired a supercomputer with a computing capacity equivalent to 34,000 laptops.[2]

We are in the midst of a digital revolution, and it's likely that the biggest changes still lie ahead of us. With the emergence of faster networks (5G), more of the objects around us, such as our cars, fridges and running shoes, will be equipped with computers. A new ecosystem has emerged: the internet gathers data, both online and in the physical world (sensors, cameras, computers in things connected to the internet); data is stored in the 'cloud', which has nothing to do with little fluffy cotton balls in the sky but, rather, is a system of huge, physical data storage centres; big data[3] is processed by increasingly advanced artificial intelligence systems and forms the basis of complex calculations that can reduce waste, lower emissions, increase efficiency and make daily life simpler for us all. Soon the self-driving bus will pick you up wherever you are and depart whenever its passengers wish. In short: digital technology is altering our lives.

I have spoken with many people while working on this book.[4] Our discussions have focused on regulation of big tech companies, the development of smart cities, working conditions in the platform economy, ownership and control over data, the use of sensors and artificial intelligence, as well as new digital identification systems. A common thread in our conversations has been how digital developments are shifting the balance of power in society – and therefore altering our freedom.

It isn't just our daily lives this new technology is altering. With its surveillance, manipulation and addictiveness – not to mention issues surrounding self-determination and free will – it also poses a challenge to the boundaries of our personal freedoms. How free and independent can our choices be when algorithms control the information that we receive or when an app has more information about us than we have about ourselves? What becomes of democratic checks and ownership of decision-making when big tech companies develop solutions and gather data about us not only in our homes, on social media and in the workplace, but also in the cities we live in?

Discussions about this new technology have long been dominated by tech optimists who like to talk about all the opportunities it offers. *Techlash* is a new term for what occurs when optimism about technology begins to go into reverse. These concerns centre around concentrations of power, job insecurity, widening economic inequality, the loss of self-determination, the rise of control and surveillance, and the undermining of privacy protections. Many people are likely both anxious *and* optimistic, seeing both risks and opportunities, and most of us have questions.

In this new ecosystem it is not just computers that have become important, but streams of data too. We give away so much information about ourselves: How might it be misused? Who profits from it? How can it be put to good use? Data streams are power. Data streams are major sources of income. And since access to adequate and reliable information has always been the foundation of political control, data streams are also politics. The proper understanding and application of large volumes of data will also be one of the keys to solving the challenges we face as a society.

The United States has permitted a handful of technology companies to grow to dominance with little government interference or regulation. Over the last decade, Amazon, Apple, Facebook, Microsoft and Google (Alphabet) have congregated at the top of the pile. While many other companies hit financial woes during Covid-19, these five increased their earnings and, in June 2020, accounted for one-fifth of the S&P 500, a stock market index of five hundred large

US companies.[5] This was at the same time that Jeff Bezos (Amazon), Tim Cook (Apple), Mark Zuckerberg (Facebook) and Sundar Pichai (Google) were called in to the US Congress to answer questions on whether the companies they lead have amassed too much power.

There are large technology companies in China too, but there a handful of companies cooperate with an authoritarian government that combines centralised planning with comprehensive digital surveillance and control of its own population. The superpower has ambitions to become a world leader in artificial intelligence and new technology.

The European Union is an important market for technology companies, but here they encounter resistance. In introducing the General Data Protection Regulation (GDPR), the EU's aim has been to take citizens' privacy seriously. Google, Amazon, Apple and other technology companies have been fined or put under investigation for breaching competition rules. The EU has also drawn up a plan for dealing with the ownership of data and guidelines for the use of artificial intelligence.

The outbreak of Covid-19 in the winter of 2020 and the resultant lockdowns sped up the pace of digitalization around the world. Mobile phone apps gave people an overview of whether they had been in the vicinity of anyone who was infected. At the international level, big data was used to screen health information and to conduct research into vaccines. In Rome there were debates about whether to send out drones above the city to check if people were complying with the imposed curfew. We also had to put digital tools to use in solving the regular tasks of the state. It took only a few days for Norwegian teachers to establish online classrooms. Municipalities that had yet to offer digital solutions for social security benefit applications achieved it within weeks, and municipal councils moved their meetings onto Facebook. In the private sphere, the use of digital channels shot through the roof too, with wine evenings on Zoom and quiz nights on Teams.

In many ways, what happened during Covid-19 also reinforced the message of this book: Technology is useful in many areas of life,

but its development must be given political direction and governance in order to ensure that society tackles crucial issues at the same time as power and resources are equitably distributed. It will not be possible to exploit the technology's potential without close cooperation with the private sector or tech companies, but developments cannot occur on their terms.

We need a new roadmap for digitalization and for how our data is used. The private sector needs to put forward workable solutions. The public sector needs to propose regulations and objectives. But ordinary people like us also have a job to do. We need to think more like residents of a country, of a city, of a municipality, and less like consumers in a marketplace. Far too great a part of the discussion has centred around how we as consumers can protect ourselves against the misuse of data about us, that our data is stored properly stored and our privacy safeguarded. While this discussion is important and necessary, it is only a small part of a much bigger picture which revolves around managing technological developments to meet society's common needs. It is a task for you and for me, a task for politics, and a task for democracy.