

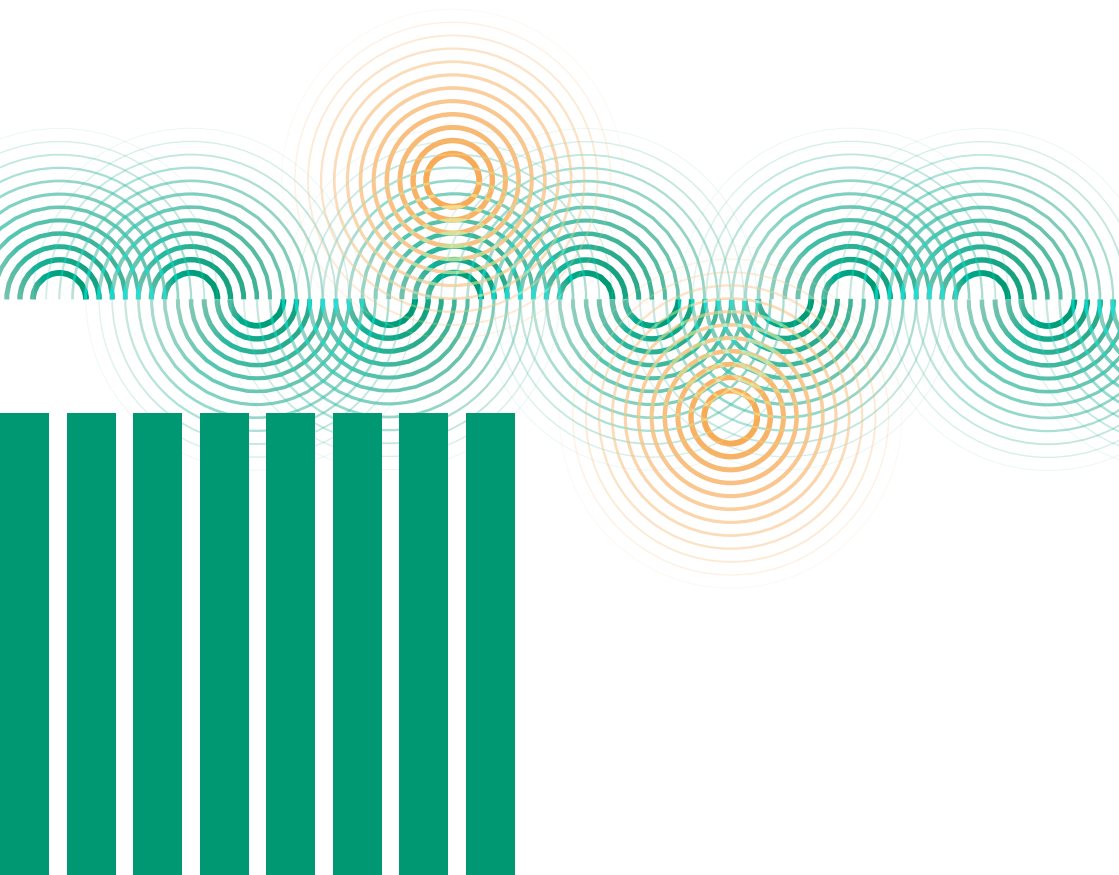
# THE ROLE OF BIG TECH AS DIGITAL INFRASTRUCTURE

Report from the government's expert group on big tech



Regeringens ekspertgruppe

**TECH-GIGANTER**



## THE ROLE OF BIG TECH AS DIGITAL INFRASTRUCTURE

November 2024

The Ministry of Digital Affairs  
Stormgade 2-6,  
DK-1470 Copenhagen

+45 72 28 24 00  
[digmin@digmin.dk](mailto:digmin@digmin.dk)

ISBN 97887-85325-05-1 (digital)  
ISBN 97887-85325-07-5 (print)

The publication can be downloaded at:  
[www.digmin.dk](http://www.digmin.dk)

Design and layout: Communication unit of the Danish Ministry of Industry,  
Business and Financial Affairs and BGRAPHIC

4	<b>PREFACE</b>
6	<b>SUMMARY</b>
12	<b>THE SEVEN PRINCIPLES FROM THE EXPERT GROUP</b>
14	<b>PRINCIPLE 1</b> <b>THERE NEEDS TO BE AN OVERVIEW OF BIG TECH'S INFLUENCE ON THE DIGITAL INFRASTRUCTURE</b>
16	<b>PRINCIPLE 2</b> <b>MAKE DATA ACCESSIBLE IN WAYS THAT BENEFIT AND EMPOWER THE INDIVIDUAL AND SOCIETY OF THE FUTURE</b>
19	<b>PRINCIPLE 3</b> <b>ALTERNATIVES TO BIG TECH'S SERVICES NEED TO EMERGE AND GROW</b>
22	<b>PRINCIPLE 4</b> <b>NO ONE SHOULD BE FORCED TO USE BIG TECH'S SERVICES TO GET INFORMATION AND PARTICIPATE IN SOCIAL, CULTURAL AND DEMOCRATIC COMMUNITIES</b>
24	<b>PRINCIPLE 5</b> <b>THE PUBLIC SECTOR SHOULD NOT BE DEPENDENT ON BIG TECH'S SERVICES</b>
26	<b>PRINCIPLE 6</b> <b>DANISH EDUCATIONAL INSTITUTIONS MUST BE FREE FROM COMMERCIAL BIG TECH</b>
28	<b>PRINCIPLE 7</b> <b>BIG TECH'S PLATFORMS MUST BE SAFE PLACES TO SHOP</b>
33	<b>COMPOSITION OF THE EXPERT GROUP</b>
34	<b>THE EXPERT GROUP'S MANDATE</b>
36	<b>SOURCE LIST</b>

# PREFACE

BY THE CHAIR OF THE EXPERT GROUP,  
**PROFESSOR MIKKEL FLYVERBOM**



Denmark has a well-developed and well-functioning infrastructure – often based on collaboration between the public and private sectors – that has created the foundation for growth, welfare and security. Infrastructure includes physical facilities and systems that provide stable access to transport, communication and public services that citizens, businesses and institutions need. Traditionally, infrastructure has been about access to things like water, electricity, roads, healthcare and educational institutions. However, today, we are also increasingly dependent on well-functioning digital systems.

Unlike other forms of infrastructure, parts of the digital infrastructure do not fulfil common principles of democratic control and collaboration between private and public players. When we refer to digital as infrastructure in this report, it is to emphasise that a large part of our communication, work life, leisure life, school life, public institutions and other important societal functions are connected to big tech's platforms, social media, apps, cloud solutions and other digital solutions. In a thoroughly digitalised country like Denmark, this dependency makes us vulnerable, especially when other forms of supply and coordination are increasingly dependent on the digital infrastructure. We see this, for example, when IT crashes at big tech disrupt air travel and hospital systems and when cyberattacks affect other forms of supply.

We have gone from a situation where it made sense to talk about the digital realm as a separate cyberspace to a situation where digital has been assigned a role as the backbone of society. When digital technology is given this central role, it is crucial to support and contribute to the democratic society we want to preserve and build.

A growing challenge is that parts of the digital infrastructure are developed, owned and controlled by big tech companies that focus primarily on technological advances, rapid roll-out and commercial gains and do not necessarily prioritise accountability, protection of children and other citizens and democratic values. Although EU digital legislation defines some rules for large tech companies, we are currently in a situation where our society has become increasingly dependent on digital infrastructures over which we have very little control. This makes us vulnerable in vital areas such as the economy, democracy and security.

The disconnection of parts of the digital infrastructure from democratic control, insight and rules is a fundamental problem. We do not accept this disconnect to the same extent when it comes to other infrastructures that our society depends on. It is difficult to imagine a situation where all other infrastructure worked in the same way as the digital one: That our water supply or road networks, for example, were owned by large global



corporations that arbitrarily set the rules, were unapproachable and prioritised profit over rights, accountability, lawfulness, security and citizen protection. Just as other infrastructures are something Danish society defines the framework for, invests in and coordinates in interaction with suppliers and other private players, we also need digital infrastructures that match our society's needs better than the current ones.

For many years, there has been a lack of political attention, societal interest and robust regulation in the digital area. As a society, we now have a greater understanding of the harmful consequences of big tech's business models and lack of accountability and protection. However, more principled and fundamental action is required if we are to avoid losing further control to big tech in a future where digital systems become even more intertwined with societal and geopolitical developments.

Many other countries, such as Sweden, Germany, France and the Netherlands<sup>1</sup>, focus on connecting the digital infrastructure to the society they want to promote by building digital infrastructures and increasing control, which requires significant investments and coordination between suppliers, authorities, public institutions and others. In return for such investments, Danish society has much to gain. This report aims to address the structural issues that make it difficult for people to

participate in cultural, social and democratic communities without being dependent on big tech. At the same time, we point out the vulnerabilities created by the public sector's dependency on big tech and the problematic situation where data are used primarily for limited, commercial purposes and not to develop the welfare society of the future. If we are to succeed in creating a breeding ground for alternatives to big tech and democratic oversight and control of the digital infrastructure, it must become a political priority and a specific long-term focus area in Denmark and the EU.

Based on its mandate's focus on the "structural issues where the big tech's business model challenges our society, culture, economy, well-being, etc.", the expert group in this report provides some principled suggestions on how Denmark can reduce its vulnerability and actively shape digital development from now. This requires that Denmark paves the way for digital infrastructures that are more in line with democratic values and less driven by the interests of big tech.

# SUMMARY

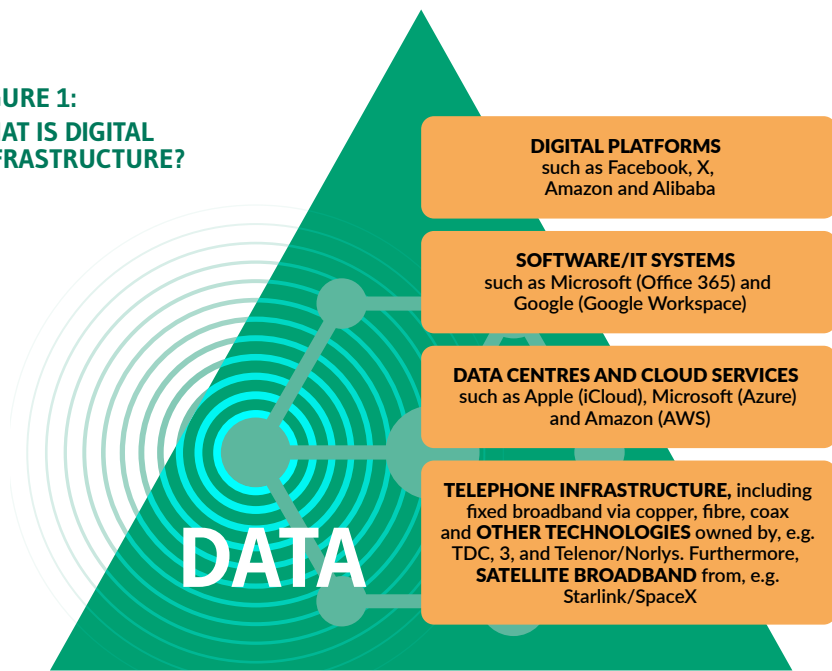
In the first two reports, the expert group focused on the issues arising from big tech's business models, commercial interests, and roll-out of artificial intelligence. The economic and technological power highlighted in the previous reports makes it necessary to also focus on the extensive role of big tech as digital infrastructure in society. The influence and societal power of big tech companies increase when their investments in infrastructure support and reinforce existing corporate power positions, such as in AI.

Denmark is one of the most digitalised countries in the world, and an ever-increasing part of society's functions and communication takes place digitally. This makes our society efficient, while also creating vulnerabilities. This is especially true if there is not enough oversight, control and thoughtfulness regarding who gets access to own and operate the digital infrastructure in a broad sense.

By looking at the digital infrastructure broadly, it is possible to clarify how big tech affects large parts of Danish society. This focus is essential to address the structural issues created by the big tech that the expert group has been mandated to work on.

Digital infrastructure is the foundation of thoroughly digitalised societies and enables the exchange of digital information between authorities, citizens and businesses. It includes everything from basic physical network infrastructure to our daily services, such as Outlook, MitID, Aula and Digital Post. It also includes the apps, websites and digital platforms used for communication, information, coordination, buying and selling. The data generated and collected when we use the Internet runs throughout the digital infrastructure. Figure 1 provides an overview of the different types of digital infrastructure covered in this report.

## FIGURE 1: WHAT IS DIGITAL INFRASTRUCTURE?



Parts of the digital infrastructure are considered *critical* digital infrastructure. Maintaining or restoring vital societal functions such as energy, drinking water, fibre networks, and mobile networks is necessary. Critical infrastructure is often subject to legislation to ensure availability, stable operation and supply, among other things. Some critical infrastructure is also subject to economic regulation to ensure efficient operation and reasonable consumer prices, which applies to water supply, for instance. There may also be a requirement for the geographical location of

critical infrastructure in Denmark. For example, the Danish Data Protection Act and the Danish Enforcement Act<sup>2</sup> contain such a location requirement.<sup>3</sup> The purpose is that Danish authorities have access to the IT systems in question and the opportunity to counteract the unauthorised use of personal data in the system within the legal framework, among other things. The location requirement covers systems such as MitID, the Civil Registration Number (CPR) register and Digital Post.

## INFRASTRUCTURE REGULATION AND CYBERSECURITY

### DANISH INVESTMENT SCREENING ACT

Critical infrastructure is subject to the Danish Investment Screening Act, which means that foreign investments, etc., in companies within critical infrastructure, require prior authorisation.<sup>4</sup> The purpose is to prevent certain companies from operating or developing critical infrastructure in Denmark if there is a risk that the activity can be exploited for, e.g. espionage. For instance, in May 2023, the Danish Business Authority refused to approve NKT's divestment of a subsidiary under the Investment Screening Act.<sup>5</sup> As of 1 July 2023, the act has been significantly expanded, in light of new geopolitical shifts, increased superpower competition and Russia's invasion of Ukraine, which has significantly increased the security threat to Denmark and Danish critical infrastructure in recent years.<sup>6</sup>

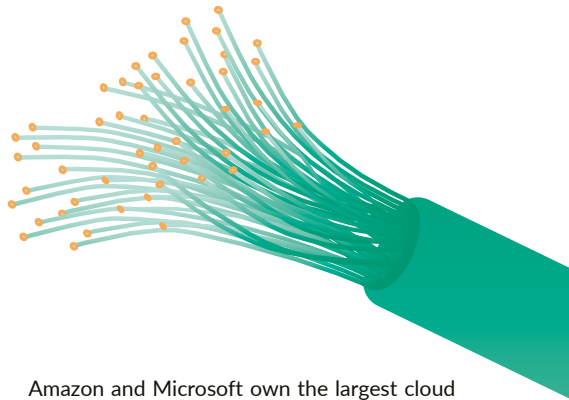
### NIS2 AND CER

The Cybersecurity Directive (NIS2) aims to ensure that companies and authorities in the EU that are part of essential or critical infrastructure achieve a high common level of cybersecurity.<sup>7</sup> This includes stricter requirements for management, minimum requirements for managing cybersecurity risks, requirements for notifying authorities of security incidents within specified deadlines and fines for violations. The Critical Entities Resilience Directive (CER)<sup>8</sup> aims to strengthen the resilience of critical infrastructure to physical threats, such as natural disasters, terrorist attacks, insider threats or sabotage. For example, if a company or organisation is characterised as a critical infrastructure, procedures are required for background checks on people who perform sensitive tasks or have access to company premises, information or control systems.

### CYBER RESILIENCE ACT

The Cyber Resilience Act aims to ensure a minimum level of cybersecurity for digital products in the EU so that they have fewer vulnerabilities when they are placed on the market and receive continuous software updates. At the same time, it should make it easier for consumers to understand the cybersecurity of products and use them safely. With the regulation comes pan-European cybersecurity requirements for anyone who manufactures, develops and imports products with digital elements, including both software and hardware.<sup>9</sup>





Furthermore, it has been decided that, in some cases, the Danish state should have ownership of certain companies to fulfil a need to control critical infrastructure.

There is also infrastructure that is not currently defined as critical and, therefore, not regulated in the same way. However, it still plays a vital role in our society. This report focuses on the role of big tech as – and influence on – digital infrastructure in a broad sense.

Big tech companies own various parts of the digital infrastructure in Denmark and Europe. Big tech companies like Alphabet and Meta provide the most used websites and apps, collect large amounts of user data and invest in infrastructure such as data centres.<sup>10</sup>

Amazon and Microsoft own the largest cloud services, and SpaceX – owned by Elon Musk – will provide fast satellite Internet to Molslinjen ferries in Denmark<sup>11</sup>. Google and Meta are part of a consortium that will build a transatlantic undersea fibre cable of over 7,000 kilometres between Esbjerg and New Jersey in the US.<sup>12</sup>

Big tech's services are also used in large parts of the public sector: Chromebooks in municipal primary and lower secondary schools, iPhones and iPads in ministries and agencies, and municipalities, and the costs to Microsoft for using their cloud service, among other things, are increasing. Moreover, there is a layer of search engines, social media and marketplaces – owned by the big tech – that act as digital infrastructure for information, conversations, buying and selling.



## THE EXPERT GROUP'S UNDERSTANDING OF BIG TECH

The expert group did not work with a fixed definition of “big tech” – to avoid focusing on named companies. Instead, the expert group has used a looser definition: Technology companies that, through the roll-out of their platforms and services, have achieved a unique and, in some cases, dominant status in key areas of society and, therefore, impact users' fundamental rights. These are companies that, to varying degrees, base their business model on collecting huge amounts of data for use and dissemination to third parties who use the information for advertising, for example.

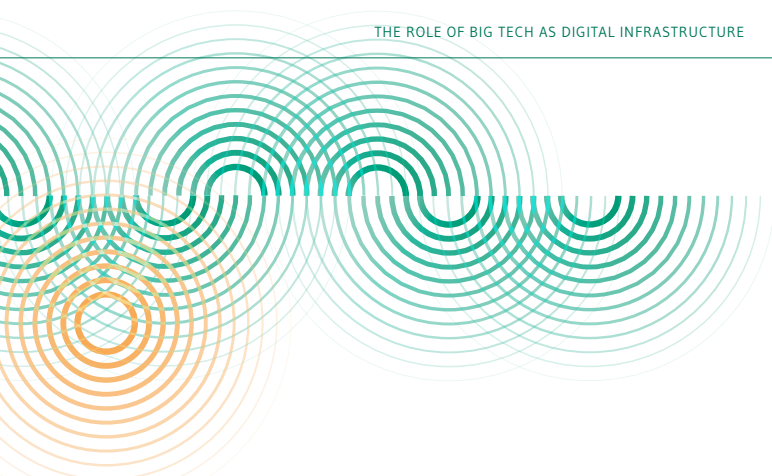
The ownership and influence of big tech makes Denmark vulnerable. The vulnerability arises from three types of challenges: economic, democratic and security.

*Economic* vulnerabilities arise when we become dependent on big tech companies who gain a market power that cancels out effective competition. Effective competition ensures lower prices, higher quality and a wider range of products and services. Dependency makes negotiations such as pricing more complex and can lead to overpaying or accepting terms that would otherwise not be accepted.

*Democratic* vulnerabilities arise when big tech companies, for commercial or other reasons, challenge or attempt to circumvent the rules and rights decided by our democratically elected politicians and the decisions made by authorities. It is also a democratic challenge if there is no transparency about the big tech's influence through, for instance, donations to municipalities, schools, universities and think tanks.<sup>13</sup> Finally, democratic discourse and access to credible content are challenged when big tech's algorithms determine the content users see on their services based on commercial considerations, and the big tech will not disclose which posts are promoted or removed and why.

*Security* vulnerabilities arise when big tech companies become so powerful that they can exercise a form of foreign and security policy and become part of geopolitical tensions. A recent example is Elon Musk, the owner of X, whose Starlink satellites have played a crucial role in the war in Ukraine.<sup>14</sup> This example illustrates how big tech conducts its own foreign and security policy through an individual. Another example is TikTok, which collects vast amounts of data about its users. They are used for espionage, blackmail, etc.<sup>15</sup> Finally, through their services, big tech can influence elections, amplify tensions and conflicts and cast doubt on the facts behind political decisions. There are also other security vulnerabilities regarding critical infrastructure, such as the risk of hacking, cyberattacks, physical sabotage and the like. These cybersecurity vulnerabilities form part of the backdrop for this report but will not be described in detail.

Both Denmark and the EU focus on the need to strengthen and regain "digital sovereignty"<sup>16</sup>, i.e. reduce political, economic and technological dependency on specific companies and countries to reduce our vulnerability, protect democratic values and security interests and strengthen European competitiveness.<sup>17 18 19</sup>



The EU plays a key role in ensuring that rules are set, enforced and respected. Effective implementation and enforcement of the regulation are crucial to this role, which is especially true of the recently enacted EU regulations, such as the AI Act, Digital Services Act, Digital Markets Act, Data Act, and Data Governance Act. However, the expert group believes more must be done to increase democratic control.

In this report, the expert group offers suggestions on what society's digital infrastructure could look like if we want to increase democratic control, and what benchmarks we can aim for to get there. It is very much about what *can be built* and *used as alternatives* to the big tech's services and what rules big tech must play by. This is necessary to address the structural issues the expert group has been mandated to work on, primarily caused by big tech's business models.

The report presents seven principles that the expert group recommends be used when making future decisions about the role of big tech in Danish society. By following the principles, it will be possible to address many of the challenges of the big tech that the government has mandated the expert group to address. This ensures responsible technological development that supports Denmark's democracy, prosperity and security in a globally connected world.

The first three principles are about how we want the digital infrastructure to be organised in the future. There needs to be more control over big tech, and we need to support alternatives and ensure that data empowers the individual and society of the future. The last four principles focus on different parts of Danish society and describe the principles that should govern the influence of big tech.

# THE SEVEN PRINCIPLES FROM THE EXPERT GROUP

1

**THERE NEEDS TO BE AN OVERVIEW OF BIG TECH'S  
INFLUENCE ON THE DIGITAL INFRASTRUCTURE**

2

**MAKE DATA ACCESSIBLE IN WAYS THAT BENEFIT AND  
EMPOWER THE INDIVIDUAL AND THE SOCIETY OF THE FUTURE**

3

**ALTERNATIVES TO BIG TECH'S SERVICES NEED  
TO EMERGE AND GROW**

**4**

**NO ONE SHOULD BE FORCED TO USE BIG TECH'S SERVICES TO GET INFORMATION AND PARTICIPATE IN SOCIAL, CULTURAL AND DEMOCRATIC COMMUNITIES**

**5**

**THE PUBLIC SECTOR SHOULD NOT BE DEPENDENT ON BIG TECH'S SERVICES**

**6**

**DANISH EDUCATIONAL INSTITUTIONS MUST BE FREE FROM COMMERCIAL BIG TECH**

**7**

**BIG TECH'S PLATFORMS MUST BE SAFE PLACES TO SHOP**

# PRINCIPLE 1

## THERE NEEDS TO BE AN OVERVIEW OF BIG TECH'S INFLUENCE ON THE DIGITAL INFRASTRUCTURE

### GUIDELINES

- a. There is a publicly available overview of the ownership structure of the digital infrastructure. The overview is continuously updated, and ownership is monitored.
- b. Alliances have been formed with like-minded countries to promote European investment and collaboration in developing digital solutions that support the democratic rule of law.
- c. A wider range of high-quality cloud solutions and AI models are available in Denmark and Europe.



Big tech companies play vital roles in and as digital infrastructure in Danish society. Google and Meta provide the most used websites and apps, collect large amounts of user data and invest in data centres, for example. Microsoft products are the most widely used for word processing and email in government and regulatory offices around the world. Aula is hosted by Amazon Web Services (AWS).<sup>20</sup> Governments and public authorities sometimes depend on big tech to fulfil key national security tasks. For example, the UK government signed a deal with Amazon in 2021 to host cloud data from all their intelligence agencies and the Ministry of Defence.<sup>21</sup>

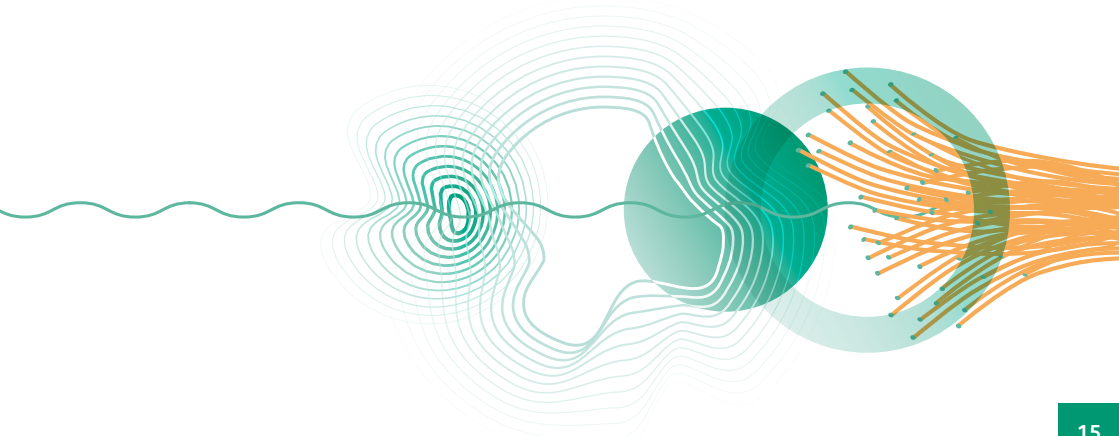
In Denmark, parts of the digital infrastructure previously in Danish hands are now in foreign hands. Key parts of the Danish payment infrastructure are still owned by Danmarks Nationalbank, i.e. the Danish state. However, for example, Dankort is now owned by Nets, which the Italian Nexi Group has acquired. Nets has sold its direct debit service (Betalingsservice) to Mastercard. The ownership of Nets has changed over time through mergers and acquisitions. From being bank-owned under the name Pengeinstitutternes Betalings Service, Nets is now owned by an Italian company, which in turn is owned by several foreign equity funds.

Complex ownership structures are constantly changing, which raises the question of whether there is a sufficient overview of who owns and operates the digital infrastructure and digital solutions that essential parts of society are built on and dependent on, not only in case of supply crises but also in terms of the ongoing impact that ownership can have on Denmark. Finally, there is a risk that ownership may prioritise commercial interests over, for example, data security and operating reliability. For instance, earlier this year, Nets was heavily affected by a DDoS attack, which is a simple and old-fashioned hacker attack.<sup>22</sup>

Big tech is also gaining a foothold in the payments infrastructure market. Figures from 2022 show that more than one in five consumers used a digital payment solution for their last payment in a physical shop. Apple Pay was used by approximately 10 per cent of consumers for their last payment.<sup>23</sup> Today, most customers pay with the Visa or Mastercard portion of their card when using Apple Pay. Most Danish banks have not integrated Dankort into mobile payment solutions like Apple Pay.<sup>24</sup> At the same time, until recently, it was not possible for Apple's competitors to access the contactless NFC chip in iPhones. Apple has stated to the European Commission<sup>25</sup> that they are working to enable the likes of Vipps, MobilePay and Nets to develop competing payment solutions for Apple Pay. However, it is not yet clear what terms Apple will set for usage.<sup>26</sup>

The fact that more and more of our lives and key societal functions are digitalised is a considerable strength. However, it also creates economic, democratic and security challenges. The widespread use of big tech's digital infrastructure, combined with severely limited access to big tech's engine rooms and decisions, can create dependencies and lead to vulnerabilities. Big tech may have economic interests that do not align with societal values and may be subject to states that do not wish Denmark well. If the digital infrastructure is operated without Danish authorities or the public having adequate access to and influence over the engine room, society loses the ability to monitor and identify potential risks and vulnerabilities and thus take the necessary measures to ensure democratic control.

In the future, even more parts of society will depend on and connect to digital solutions, which makes infrastructure control crucial. There is currently no public overview of the ownership of the type of digital infrastructure that the expert group addresses in the report. The expert group believes there must be an overview and control of the digital infrastructure that is the foundation of society and the Danish business community, which will require close and effective collaboration between authorities across the state, regions and municipalities. A digital infrastructure council or body could also be established to provide transparency and advice on organising the digital infrastructure responsibly and promoting maximum democratic control.



# PRINCIPLE 2

## MAKE DATA ACCESSIBLE IN WAYS THAT BENEFIT AND EMPOWER THE INDIVIDUAL AND SOCIETY OF THE FUTURE

### GUIDELINES

- a. Big tech companies have ensured that citizens can easily export and share their data with other players clearly and securely.
- b. Increased use and support of data spaces has made it possible to share and utilise data across services for limited purposes securely and efficiently.
- c. It is easy for citizens to get an overview of what they have consented to and how they have control over how their data is shared.



Today, data is a valuable asset for citizens, businesses, and society. Data flows through all parts of the digital infrastructure and is primarily used by big tech to optimise services and products and for commercial purposes such as advertising sales and user retention. The large concentration of data in the hands of big tech companies makes them powerful because they gain great insight into users' behaviour and psychological profiles. This knowledge is valuable in marketing, but it can also be misused to manipulate populations, for example.

The data collected is of far too little benefit to the individual and society. Users often cannot benefit from their data themselves because it resides in closed silos and often with big tech.

One of the reasons for this is that users cannot easily use data collected by one service on a new service. Users have access to their specific data with each player but cannot utilise the full potential of their collective data.

This means that citizens cannot benefit from their data across different services and cannot get a comprehensive overview of their data. For example, it could create better and more personalised healthcare treatments if citizens could allow the healthcare service to receive and use citizens' self-collected data from smartphones, smartwatches, heart rate monitors, etc.<sup>27</sup> The closed silos can also limit innovation and development of alternative services that can create value for the individual and society, as access to data is limited and fragmented.





## REGULATION THAT STRENGTHENS ACCESS TO DATA

### GDPR

The GDPR (General Data Protection Regulation) has been in effect since 2018 and contains a wide range of requirements that must be met when processing personal data. The data protection rules contain a wide range of rights for the data subject, including the right to know what data a controller is processing about them and the right to data portability, i.e. certain options for the data subject to transfer personal data about themselves from one data controller to another.

### DIGITAL MARKETS ACT

The Digital Markets Act sets requirements for big tech, such as what data companies using a gatekeeper's service should have access to. This data can allow companies to understand market trends and consumer behaviour in more depth and help companies improve their own products and services. All of this can help Danish and European companies challenge the entrenched position of big tech in certain markets.

### DATA ACT

The Data Act is designed to promote access to and use of data. At its core, the act will make it mandatory for providers to share data generated using a product or related service ("The Internet of Things (IoT)") with the user. This means that individuals and companies have the right to access data they generate when using products or services. In addition, the act establishes rules for data processing services, such as cloud services, to make it easier for users to switch between data processing services. It also establishes a framework for data-sharing agreements to protect micro-enterprises and SMEs from unfair contractual data-sharing terms. The act introduces measures to protect against unauthorised access to non-personal data by third parties in the EU. As part of the act, standards will be developed to support data sharing across sectors.

### DATA GOVERNANCE ACT

The Data Governance Act is designed to create a framework for secure, fair and open data exchange in the EU. One of the primary goals of the act is to facilitate data exchange across public and private sectors and between Member States and EU institutions. The Data Governance Act will promote data sovereignty and control over data for EU citizens and businesses to strengthen the EU's position in the global data economy. It also calls for increased data sharing in the EU, especially in health, environment and industry sectors, to drive innovation and growth. The act also includes data protection provisions to ensure data security and privacy rights are respected under the GDPR.

The Digital Markets Act gives users of big tech's platforms more options to control data collection and use, for example, by making it possible to opt out of big tech combining users' data across their platforms.

However, many users still do not have easy access to and control over data. At the same time, users lack opportunities to effectively access their data and choose whether to make it available to researchers, the public sector or private companies that can use the data to solve challenges such as climate change, health issues and the like.

One way to share data is using common European data spaces. Data spaces aim to create a secure and trustworthy infrastructure for sharing data across many players, sectors and countries. The infrastructure should make it easier and more transparent to grant access to data for specific purposes. The expert group supports the EU's ongoing work on data spaces.

The expert group believes that the benefits and gains that can be realised from secure and efficient data sharing should be highlighted, which applies to citizens, Danish society and businesses alike. Therefore, supporting effective implementation of the Digital Markets

Act, Data Act and Data Governance Act is essential. It will also be relevant to require data localisation in the EU in many areas related to digital infrastructure to ensure that data stays in Denmark and Europe. The requirement may also mean that cloud providers, for instance, must have their legal headquarters in Europe.

The expert group also believes that an important focus should be to inform Danish citizens about their right to have their data moved, their options to use this data for good purposes, and their right to complain if their rights are not respected. Here, you can take inspiration from the Danish non-profit organisation Data for Good Foundation. Through the Data for Good platform, citizens get better control and overview of their data and can share it when it makes sense. At the same time, an ecosystem is created where data can be anonymously transformed into new knowledge to benefit individuals, companies and the public sector.<sup>28</sup>

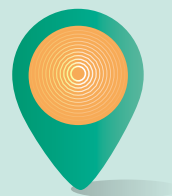
One area where it will be relevant to strengthen public datasets is described in the National Plan for Motion Data,<sup>29</sup> where the public sector can use satellites and data to support innovation and independence from big tech in a growing mobility market.

# PRINCIPLE 3

## ALTERNATIVES TO BIG TECH'S SERVICES NEED TO EMERGE AND GROW

### GUIDELINES

- a. Denmark and like-minded countries are paving the way for the building of digital infrastructures focusing on accountability, security and democratic control.
- b. There is a Digital Single Market with favourable conditions for investment in European tech companies to boost competitiveness through innovation, research and technological development.
- c. It is easier for tech entrepreneurs and companies to raise venture capital in Denmark and across the EU, for example, for IPOs and to grow and stay within EU borders.
- d. The European Commission prioritises the enforcement of competition rules and the Digital Markets Act against big tech.



Big tech has grown so big that they have become indispensable to businesses, governments and citizens in many areas. We rely on them to communicate, interact and trade with each other digitally. At the same time, big tech's market dominance has a negative impact on effective competition and innovation, making it difficult for alternative services to gain a foothold. Lack of competition means prices are higher, and fewer choices than in a situation with well-functioning competition.

Big tech companies like Amazon and Google can rank, promote or exclude certain content

because of their position, which can significantly impact which companies have the best chance of reaching their customers and the range of products and services consumers are presented with. Big tech can also play a dual role; for example, some operate a marketplace where independent sellers can sell products directly to consumers, while the platform itself also sells products as a retailer and competes with these independent sellers. This dual role provides access to a wealth of knowledge and large data sets about the activities of independent sellers on their platforms, which big tech companies can utilise to their advantage in areas such as product development, product



## CLOUD SERVICES

When data is stored in a cloud service, users can access their data from any device with Internet access. At the same time, it allows companies to utilise huge amounts of data and computing power without investing in and maintaining their own servers. Instead of maintaining their servers and infrastructure, businesses and individuals can purchase access to cloud services from third-party providers. Although cloud data is typically encrypted, it still held by a private company, which has some form of control over it. It also matters where the company has chosen to physically locate the data, as the physical location may be subject to national legislation that allows authorities or intelligence services access to data, which applies whether they are in China or the US.



placement and pricing. Finally, big tech's terms play a crucial role for the companies that use the services to reach their customers. In autumn 2023, Booking.com was criticised for not paying hotels on the platform on time, which challenged the finances of many small hotels.<sup>30</sup>

The few dominant players in cloud services, with Amazon and Microsoft, in particular, holding large parts of the market, means that businesses, public authorities, and organisations have limited choices, which can mean that competition is ineffective, and prices are higher than they would otherwise be.

The big players in the cloud market have a significant advantage in developing and operating AI, such as the big language models. Training and operating AI requires huge amounts of data and considerable computing power, and cloud services are an ideal infrastructure, which can both give big tech a competitive advantage and impact other companies' opportunities. There have been several examples of big tech partnering with new players in AI, such as Microsoft's partnership with OpenAI<sup>31</sup> and French Mistral<sup>32</sup>.

Big tech's strong position across markets may be because there are no equal quality or price alternatives. It is difficult for other companies to compete with the big tech due to network effects and big tech's large amounts of data and financial advantages. The new Danish supercomputer, for which the Novo Nordisk Foundation and the state fund EIFO have granted DKK 700 million, appears to be a minimal investment compared to the investments that big tech can make in AI. Meta has previously indicated that by 2023, it would spend DKK 225 billion just on developing its

AI capabilities.<sup>33</sup> At the same time, it can be difficult for smaller companies to raise the necessary capital and attract the best developers. Big tech regularly acquires small companies before they become serious competitors. Several reports indicate that Europe's competitiveness, especially in the digital area, is challenged and requires new initiatives.<sup>34</sup>

The big tech's market dominance creates vulnerabilities and can affect Denmark's autonomy and economy. Therefore, it is vital that the role of big tech is challenged. Denmark and like-minded countries can pave the way for building alternatives to the big tech, such as through business regulation, increased competition, procurement rules, investments and public-private partnerships. This requires Denmark and the EU to focus on making it easier for entrepreneurs to start and scale their businesses and introduce active control of mergers and acquisitions. Stronger interaction between universities and the business community can also help create growth, and there must be better opportunities for IT entrepreneurship for researchers and students.<sup>35</sup>

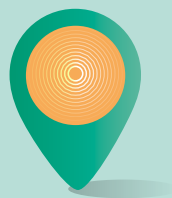
In addition, tech entrepreneurs should be able to raise venture capital more easily in Denmark and across the EU, for example, for IPOs and growth. It could also be considered whether government investments from, for instance, EIFO, Innovation Fund Denmark and pension funds should focus more on Danish startups.

# PRINCIPLE 4

## NO ONE SHOULD BE FORCED TO USE BIG TECH'S SERVICES TO GET INFORMATION AND PARTICIPATE IN SOCIAL, CULTURAL AND DEMOCRATIC COMMUNITIES

### GUIDELINES

- a. Politicians and public organisations use multiple channels for information and communication.
- b. Public debate occurs on services within a framework that ensures everyone has a voice.
- c. A free and diverse media industry and strong public service support democratic discourse.



Many citizens, organisations, institutions, companies and politicians find that they need to be present on big tech's services to get information, interact and communicate with the outside world, and participate in democratic discourse. This supports big tech's business models, which are based on retention and collection of user data, cf. the expert group's report on business models.

Social media allows politicians, experts, debaters, etc., to communicate directly with citizens. It increases the transparency of political work. Social media also allows citizens to express their views, receive information and participate in discussions. At the same time, many authorities communicate via social media to reach citizens effectively, and

political and democratic discourse takes place on social media in addition to traditional media.

Social media has also become an easy tool for many organisations, including sports clubs and other communities, to communicate widely, strengthen the community around the association or group, and recruit new members. Finally, young people use social media to communicate with their friends, coordinate activities and share big and small things.

When social media plays a major role in people's everyday lives, it can lead to democratic and security vulnerabilities. Part of the challenge is that the premise of publicity and

democratic discourse, where everyone can, in principle, have a voice and be visible, is challenged by the practices of big tech. Research shows that with big tech's algorithms, not everyone has a voice or is visible. On the contrary, emotional or provocative content gets faster interactions from other users and is therefore disseminated more than neutral content.<sup>36</sup> There have also been several examples of Danish politicians having their social media profiles blocked or having posts removed even though the contents were not illegal or disseminated misinformation – even during election periods.

With social media being such an integral part of Danes' everyday lives, it is a challenge for those citizens who do not want to be present on the platforms. This can push citizens to have profiles on certain social media platforms such as Facebook and Snapchat if the primary communication with friends or the coordination of local sports clubs' activities occurs there. Therefore, citizens do not have a real option to opt out of the services, even if they want to be free from the big tech's data harvesting.

When governments are on social media, they can reach many citizens quickly. Other channels often do not have the same reach. However, this can be problematic if citizens are unaware of it and cannot use other “official channels” for information from public authorities, the police, and emergency services. This is partly because the social media connection goes through a private company that can suddenly choose to restrict or shut down access.

Today, many people – especially young people – get much of their news through social media, and these services influence what news citizens are presented with and how. Many news stories on the platforms do not come from traditional news media or journalists subject to editorial responsibility. There are also examples of well-known, credible journalists

and media outlets having their names misused for social media scams, which can reduce access to real and relevant social information, undermine trust in established media, and increase the risk of *fake news* when news is disseminated without critical journalism and fact-checking.<sup>37</sup> At the same time, big tech companies are taking an increasing share of total advertising revenue at the expense of traditional media,<sup>38</sup> which contributes to weakening diversity in the media market.

The above illustrates some of the democratic, security and economic vulnerabilities that the role of big tech creates. The expert group believes that big tech companies in their current form cannot take on the role of dominant digital infrastructure to safeguard democratic discourse, community life and news dissemination.

The expert group believes it should be possible to follow and participate in democratic discourse without using big tech's services. When interaction occurs primarily through social media, the platforms' algorithms, features and characteristics can affect democratic discourse, communities and the functioning of civil society. Therefore, the expert group believes that politicians, for example, are responsible for using other channels, including their own websites and Danish media, and not just the major social media channels, when communicating with citizens.

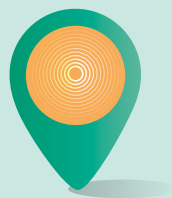
It is also important to consider how to ensure democratic participation and public debate, including allowing for diverse views. For example, by considering whether media support can be improved and made more platform- and technology-neutral by adapting it to media development and the digitalised and globalised media landscape.

# PRINCIPLE 5

## THE PUBLIC SECTOR SHOULD NOT BE DEPENDENT ON BIG TECH'S SERVICES

### GUIDELINES

- a. The public sector uses secure and responsible services and software that reflect Danish and European values.
- b. The public sector has the right skills to procure and work with alternative services and software, such as open source.
- c. The public sector is not dependent on big tech and avoids being locked into one provider by emphasising interoperability and open source in digital solutions.
- d. When it makes sense, the public sector creates smaller and more compartmentalised public tenders to enable smaller players to participate.



Many public institutions and municipalities use big tech's services, such as Office Suite, Windows operating system, and Apple's iPhone and iPad. If the public sector primarily utilises the services of big tech without considering possible alternatives, it can support and expand the strong position of big tech, reduce competition, increase dependency and thus make institutions vulnerable. At the same time, situations can arise where it is difficult to switch away from big tech's services – even in situations where prices are rising. Since 2018, municipal spending on Microsoft licences has increased from DKK 313 million to DKK 538 million, which is also related to the increasing use of function-

nalities.<sup>39</sup> This is an example of a financial challenge related to the role of big tech in the digital infrastructure.

Big tech's services can also create security vulnerabilities for the public sector, for example, when it comes to espionage.<sup>40</sup> In many countries, including Denmark, public authorities and many private companies have banned TikTok on work phones in the past year. The criticism is twofold. It addresses both the risks of China's access to data and concerns about the vast amount of data collection that is taking place. In addition to the security vulnerabilities created by big tech,



criticism has also been levelled at the lack of satisfactory IT security in public IT systems and the fact that several government authorities do not meet the minimum technical requirements for IT security.<sup>41</sup> However, this is outside the mandate of the expert group.

Part of the explanation for big tech's position is that public tenders are sometimes so large that only the biggest companies have a good chance of winning the contracts, which was the case, for example, when KL and KOMBIT wanted to develop a single IT system for all municipal nurseries, kindergartens, after-school centres and schools (Aula). Large providers can offer a better consistency of supply, and they typically have more resources and knowledge. However, in the case of the Aula tender, for example, the large, unified tender meant that earlier and smaller service providers that had some functional overlap with Aula found it difficult to participate and could not provide local and customised solutions, and so their business base was challenged.<sup>42</sup>

In Denmark, there are examples of the public sector trying to become independent of big tech's infrastructure by utilising and strengthening Danish alternative solutions. GovCloud, for instance, is the cloud solution the Agency

for Governmental IT Services uses. The intention is to offer authorities a secure cloud-based operating platform built on open source. Applications and data in GovCloud will always be in the Agency for Governmental IT Services' data centres in Denmark. There is also the OS2 community, which is a collaboration between public authorities that want to create, share, and maintain open-source solutions with the help of private IT providers.

To gain more control and strengthen prosperity, democracy and security, the public sector must take the lead and choose alternatives to big tech, such as cloud services and artificial intelligence systems. Focus should be on data protection, data ethics, interoperability and open source.

Such requirements should also be included in public tenders, cf. the expert group's previous recommendation 4.2. on AI. Inspiration can be drawn from the German state of Schleswig-Holstein, which has left Microsoft in favour of LibreOffice. As an experiment, three pilot municipalities could be appointed in Denmark to receive financial and professional support in switching to alternatives to big tech's products for inspiration and experience sharing with other municipalities.

## AI ACT

The AI Act (the act on harmonised rules for artificial intelligence) came into force on 1 August 2024. The AI Act is the first binding regulation for using AI worldwide. The act bans AI with unacceptable risks, such as certain types of facial recognition. The AI Act also sets requirements for high-risk artificial intelligence, such as recruitment or public case management. The act also includes a transparency requirement to inform users that a product or service uses AI, such as chatbots, or whose content is generated with AI, such as deepfakes.

# PRINCIPLE 6

## DANISH EDUCATIONAL INSTITUTIONS MUST BE FREE FROM COMMERCIAL BIG TECH

### GUIDELINES

- a. Educational institutions' digital tools are age-appropriate, ad-free, and tracking-free, and they do not use children's data for commercial purposes.
- b. Using digital services should not require the creation of personal accounts that pull pupils and students into the ecosystem of big tech.
- c. Municipalities make greater use of Scandinavian and European collaboration, learning and teaching tools.



A crucial cornerstone of Danish society is our educational institutions and municipal primary and lower secondary schools, which most Danes attend. They instil values in young people such as trust, dialogue, collaboration and open-mindedness. Therefore, we must be conscious of who we give access to this space.

Today, big tech has widespread access to children's and young people's data, which happens through the social networks that children are on, such as chat apps, online games, etc. However, it can also occur in the classroom and at the educational institutions that young people attend.

Tools such as Google Workspace for Education, Microsoft 365 for Education<sup>43</sup> and the

iPads and computers students are given and use, are part of the digital infrastructure because of their importance to education and their role in facilitating communication between students and teachers, among other things. On average, 15-year-old Danish school students use digital tools for 3.8 hours a day for learning activities at school.<sup>44</sup> You cannot be a student in Denmark without encountering and being accustomed to big tech's services.<sup>45</sup>

This gives big tech companies a massive advantage in getting children and young people to use their products from an early age, which could mean that children and young people will demand the same products when they enter the education system and the labour market.

Therefore, municipalities are also offered such products at very low prices,<sup>46</sup> and in a tight municipal budget, it can be difficult for municipalities to refuse such an offer.

In recent years, the use of Google Chromebooks and the lack of compliance with data protection rules has been criticised by municipalities. The case started in 2019 when a father complained that his son's name and school were public on YouTube. Most recently, in January 2024, the Danish Data Protection Agency found that the 53 involved municipalities' use of Google Workspace did not comply with data protection rules. This was because the use involved disclosing personal data to Google for the maintenance and improvement of Google solutions or for performance measurement and the development of new features and services that the Municipal Primary and Lower Secondary School Act did not authorise. The municipalities and Google have subsequently found a contractual solution to the problem.

The expert group believes educational institutions should use ad- and tracking-free digital teaching and learning tools. As it stands, there is no overview of which apps and services are being used where and for which age groups. KL could, in collaboration with, for example, three municipalities, establish a pilot programme in schools using systems and open-source tools not owned by big tech and offer financial and professional support.

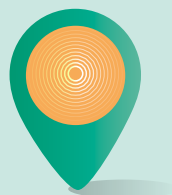


# PRINCIPLE 7

## BIG TECH'S PLATFORMS MUST BE SAFE PLACES TO SHOP

### GUIDELINES

- a. Danish companies selling products on big tech's platforms have fair terms and can engage with the platforms.
- b. Danish consumers are informed about the rights and risks of trading on big tech's platforms, such as business practices and labour conditions.
- c. Trading platforms can only operate in Denmark if the products on their platforms comply with Danish and European legislation, such as Danish product and safety requirements.



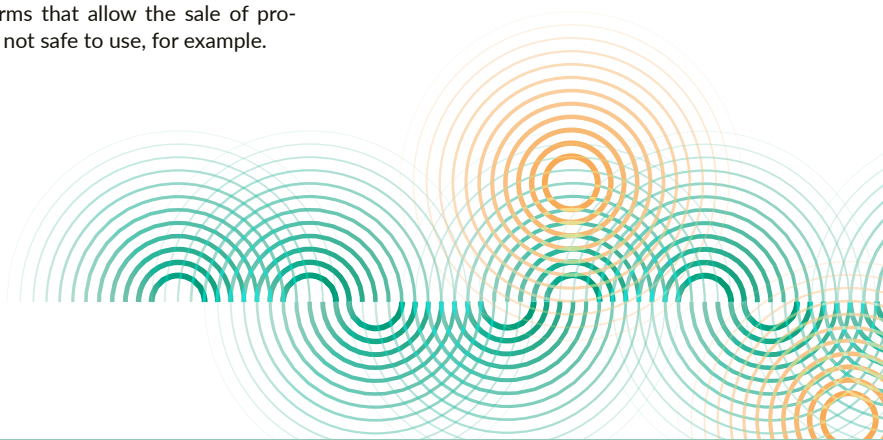
Citizens increasingly use big tech's platforms to buy everything from flights and hotel tickets to everyday products and electronics. However, it's not always the platform that the transaction is with; it is a company that sells its products via the platform. Therefore, users may find it difficult to know who to contact if there is a problem with a product or service they have purchased on the platform, such as buying flight tickets, hotel or car hire. It could also be purchasing a product on an online marketplace, such as Amazon or Temu, where the product turns out to be dangerous.

With the Digital Services Act, online marketplaces such as Amazon, Temu and Wish must fulfil some obligations, such as combating the proliferation of illegal goods. Online marketplaces must now ensure that marketplace sellers provide verified information about their identity before they can start selling their goods. Online marketplaces must also guarantee that users can easily identify the person responsible for the sale. If an online marketplace becomes aware of the seller's sale of an illegal product or service, users who have purchased the illegal product or service must be notified and informed of the seller's identity and about the option to complain.

Most recently, the Chinese big tech company Temu has attracted much attention, having recently entered Denmark with cheap products of low quality and, in several cases, the company has been found not to comply with European and Danish product regulations.

There have also been examples of Facebook and Instagram not being quick enough to remove adverts for fake websites that promise low prices but are created solely to deceive consumers.<sup>47</sup>

Therefore, the expert group wants citizens to be made more aware of both their rights and risks when shopping on platforms and for authorities to enforce regulations and have effective tools to intervene and shut down trading platforms that allow the sale of products that are not safe to use, for example.



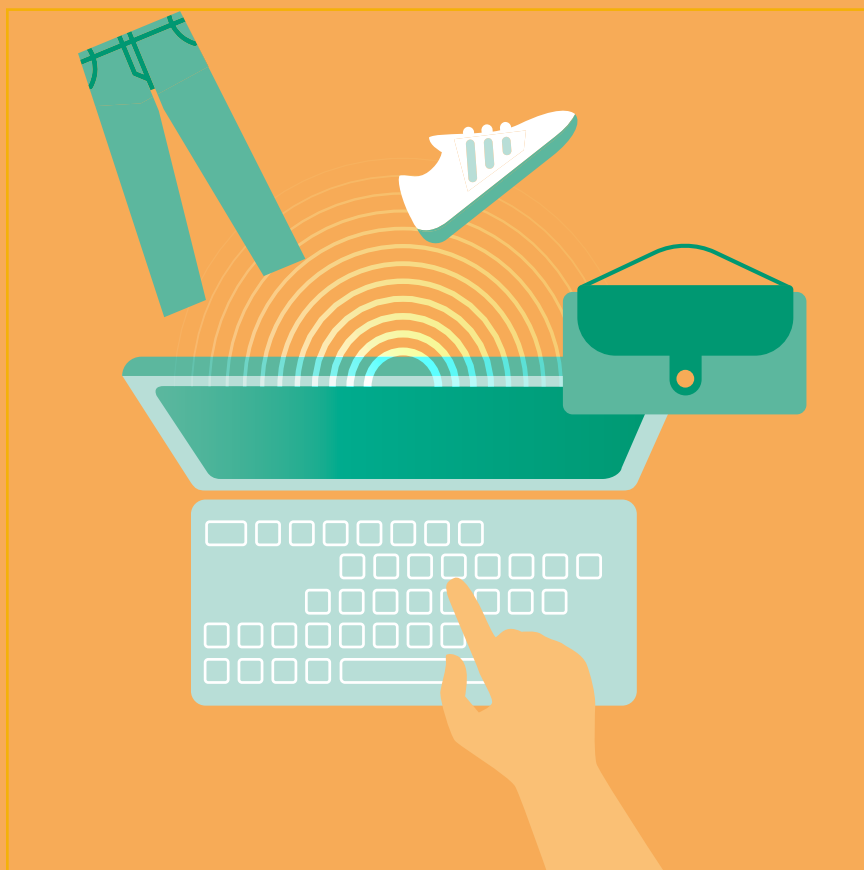
## PRODUCT LEGISLATION

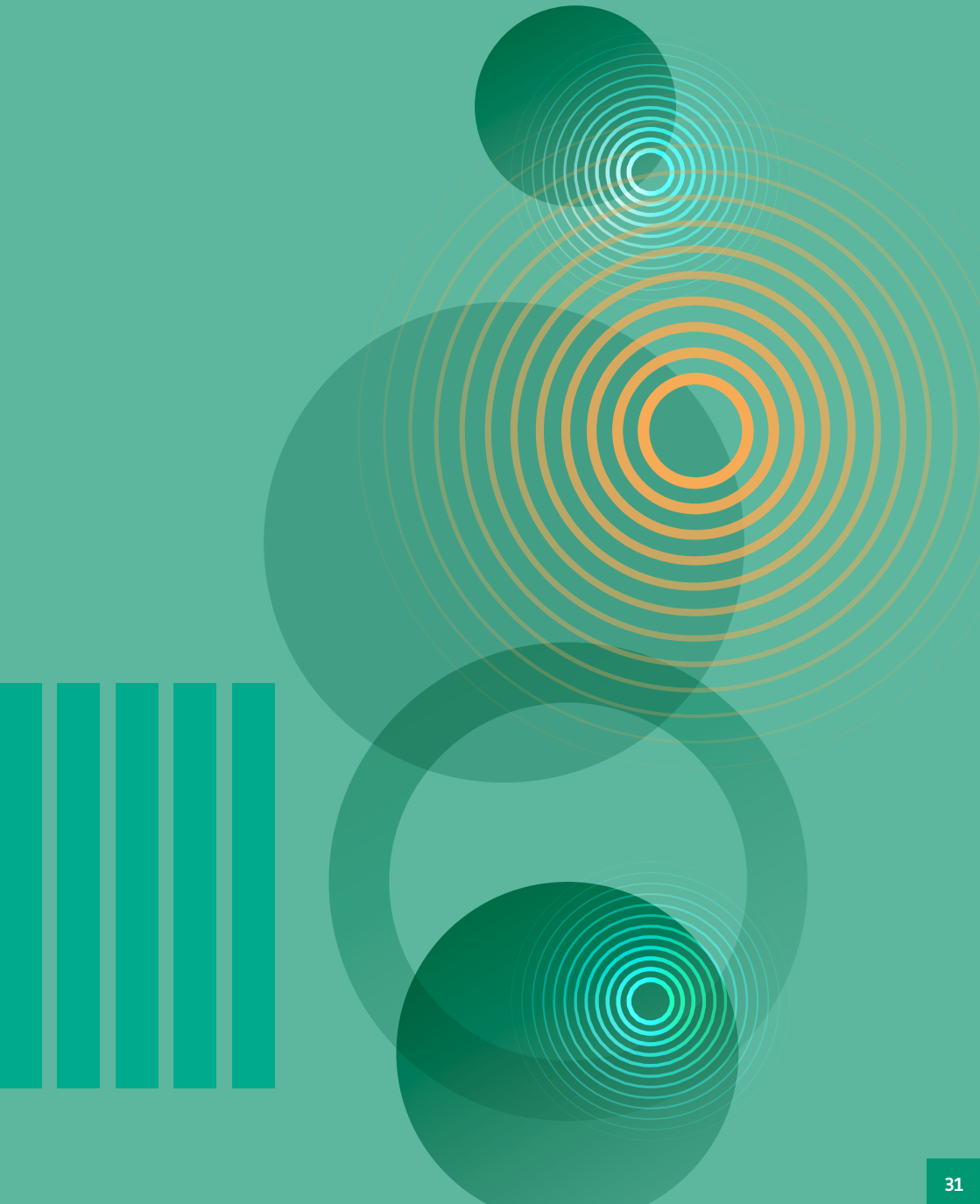
The Market Surveillance Regulation is an EU regulation establishing a common European framework for product legality and product surveillance by authorities. There are general requirements for business owners who make products available on the European market. The regulation is complemented by many EU regulations and directives that set requirements for specific types of products, such as toys, machinery and electrical products. Products marketed in Denmark and the EU must comply with product legislation, regardless of whether the products are imported by consumers directly from China or third countries.

## > LIABILITY OF DIGITAL PLATFORMS REGARDING THE GOODS SOLD ON THE PLATFORMS

The Digital Services Act gives platforms a duty to ensure that consumers can see that it is not the platform they are dealing with but a third-party seller. However, this information can be presented in many ways. In the real world, it is not always clear to the consumer whether the platform is responsible for the transaction or only facilitates the service, which can have consequences for the consumer's rights, as liability is, in principle, the seller's responsibility.

As the rules stand today, platforms are generally not liable if illegal products are sold on their platforms. However, if a platform becomes aware of an illegal product on the platform, the platform may have criminal and/or liability for damages under other legislation, such as product safety regulations, if the platform does not immediately take steps to remove the product.









# COMPOSITION OF THE EXPERT GROUP

At the time of submitting this report, the expert group consisted of the following members:

- Mikkel Flyverbom (Chairman), Copenhagen Business School
- Lars Thinggaard, Tech for Life
- Lone Sunesen, TV MIDT/VEST
- Mie Oehlenschläger, Tech & Childhood
- Miriam Michaelsen, The Media Council for Children and Young People
- Pernille Tranberg, DataEthics
- Rebecca Adler-Nissen, University of Copenhagen
- Rikke Frank Jørgensen, Danish Institute for Human Rights
- Sune Lehmann, Technical University of Denmark
- Thomas Bolander, Technical University of Denmark
- Peter Svarre, digital strategist, speaker and author

The Danish Ministry of Industry, Business and Financial Affairs and, subsequently, the Ministry of Digital Affairs served as the expert group's secretariat in collaboration with other relevant ministries, including the Ministry of Culture, the Ministry of Foreign Affairs, the Ministry of Justice and the Ministry of Children and Education.

# THE EXPERT GROUP'S MANDATE

International big tech has a huge impact on society, the economy and the everyday lives of ordinary people nationally and internationally. The Danish government has launched a number of initiatives, but there will continue to be a need for political development and new initiatives.

Against this background, as part of the government's proposal "Big tech: fairer competition and better consumer protection" from August 2021, the government will set up an external expert group. The purpose of the expert group will be to support the government's work in addressing issues related to the big tech agenda from a national and international perspective.

## Background

The consequences of big tech's development and influence have an impact on a wide range of areas, including tax, culture, and competition. Common to the big tech is that their entry into the Danish market is driven by a high demand for their services from both businesses and citizens.

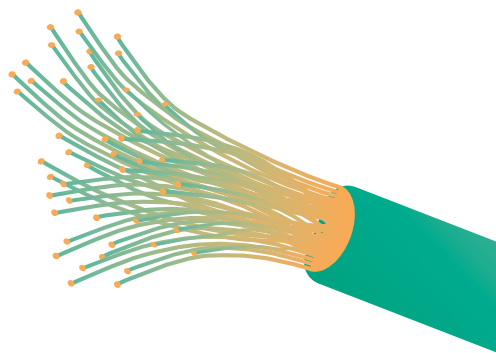
However, the presence and development of big tech also bring several challenges that are transgressive innature.

Big tech tends to operate on a business model based on collecting as much data about their users as possible. In practice, it is impossible for users to know what data they have voluntarily and involuntarily disclosed to big tech and how it is used for resale, marketing, etc.

Many of the most widespread online platforms are owned by international big tech and provide a forum for communication and public debate today. In this way, big tech has a major influence on the rules of public debate and democratic discourse.

There are also challenges related to the spread of illegal and harmful content, unfair competition, taxation, digital malaise among children and young people, opaque algorithms and polarising mechanisms. In addition, big tech is challenging decent labour market conditions, especially workers' rights.

Finally, big tech plays an increasing role in foreign and security policy in the context of the ongoing technological superpower rivalry between the US and China, which is why it will be essential to balance critical dialogue with perspectives on opportunities for knowledge sharing, innovation and collaboration.



## Task description

The expert group will serve as a forum for discussing structural issues where big tech's business model challenges our society, culture, economy, well-being, etc. Furthermore, the government will have the opportunity to ask the expert group to consider and assess specific cases and dilemmas within the tech agenda.

Specifically, the expert group will:

- Discuss the challenges of the big tech's business model and its consequences for Danish society, including democratic conversation.
- Make proposals, including highlighting possible positive as well as negative consequences, on how democratic control of big tech, with a particular focus on their business model, can be strengthened.
- Identify other issues for Danish society in light of the structural challenges resulting from big tech's business models and qualify these and their consequences for Danish society.
- Present proposals and specific recommendations for addressing these issues, including whether they should be solved at a national or EU level.
- Include and discuss international experiences in their work to ensure responsible technological development that supports Danish democracy, prosperity and security in a globally connected world.

Each departmental minister has the opportunity to request that the expert group be involved in specific issues and dilemmas within their field of responsibility.

In its work, the expert group must ensure ongoing involvement of the Data Ethics Council.

## Organisation

The chair and members of the expert group are appointed personally by the Minister of Industry, Business and Financial Affairs. The expert group is expected to consist of 12 members with expertise and experience in the big tech agenda.

The expert group is initially established for a two-years period.

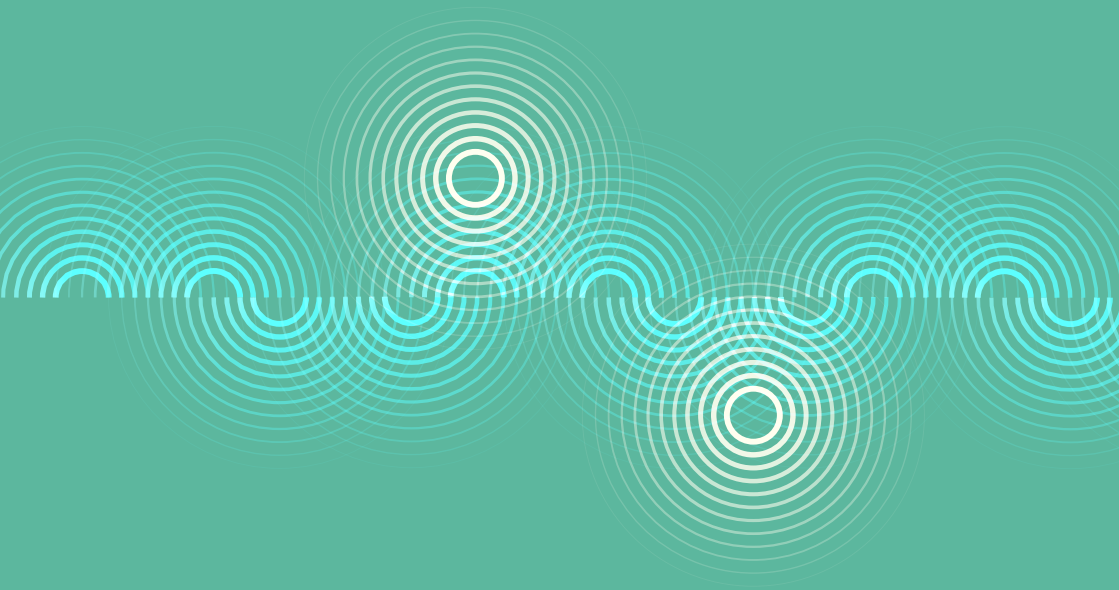
The expert group will be provided with a secretariat by The Danish Ministry of Industry, Business and Financial Affairs.

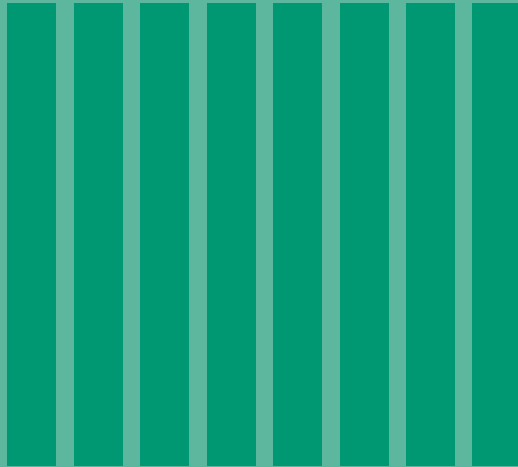
# SOURCE LIST

1. See for example <https://www.rdi.nl/radiocommunications-agency>, <https://www.digg.se/ledning-och-samordning/ena---sveriges-digitala-infrastruktur>
2. Databeskyttelseslovens § 3, stk. 9, og retshåndhævelseslovens § 27, stk. 3.
3. The Minister of Justice may order that certain IT systems operated by the public administration that process personal data may only be stored in whole or in part in Denmark.
4. Erhvervsstyrelsen, *Formål og grundlag for screening af udenlandske investeringer og særlige økonomiske aftaler*. Located on 5 November 2024 at <https://erhvervsstyrelsen.dk/formaal-og-grundlag-screening-af-udenlandske-investeringer-og-saerlige-oekonomiske-aftaler>
5. Energiwatch (2023), *NKT får afslag på frasalg af Photonics til japansk køber*. Located on 5 November 2024 at <https://energiwatch.dk/Energinyt/Renewables/article15741089.ece>
6. Investeringscreeningsloven (LOV nr 736 af 13/06/2023), *Lov om ændring af investeringscreeningsloven og lov om Klagenævnet for Udbud*. Erhvervsministeriet. <https://www.retsinformation.dk/eli/lta/2023/736>
7. Dansk Erhverv (2023), *Behov for hurtig myndighedsindsats i forhold til kommende EU-regler for kritisk infrastruktur*. Located on 5 November 2024 at <https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2023/februar/behov-for-hurtig-myndighedsindsats-i-forhold-til-kommende-eu-regler-for-kritisk-infrastruktur/>
8. CER builds on and repeals the current Directive 2008/114/EC of 8 December 2008 on European Critical Infrastructure (ECI Directive).
9. Dansk Standard, *Cyber Resilience Act*. Located on 5 November 2024 at <https://www.ds.dk/da/i-fokus/lovgivning/lovgivning-paa-det-digital-omraade-og-standarder/cyber-resilience-act>
10. Lai, S. S., & Flensburg, S. (2023), *Gateways: Comparing digital communication systems in Nordic welfare states*. Nordicom, University of Gothenburg, p. 174.
11. Ritzau (2023), *SpaceX-internet til færger i Danmark*. Located on 23 August 2024 at <https://via.ritzau.dk/pressemeddelelse/13700555/spacex-internet-til-faerger-i-danmark?publisherId=12030451&lang=da>
12. DR (2008), *Historisk: 7.000 kilometer 'Havfrue' forbinder Danmark med New Jersey*. Located on 23 August 2024 at <https://www.dr.dk/nyheder/regionale/syd/historisk-7000-kilometer-havfrue-forbinder-danmark-med-new-jersey>
13. DataEthics.eu (2023), *Big Tech Soft Power Danmark*. Located on 23 August 2024 at Big tech soft power Danmark ([dataethics.eu](https://dataethics.eu)).
14. Letter of 15 September 2023 to US Secretary of Defense Lloyd Austin from US Senators Jeanne Shaheen, Elizabeth Warren and Tammy Duckworth. Located on 23 August 2024 at [Starlink.pdf \(senate.gov\)](#).
15. Ryan, F., Fritz, A. og Impiombato, D. (2020), *TikTok and WeChat Curating and controlling global information flows*. ASPI International Cyber Policy Centre.

16. Gueham, F. (2017), *Digital sovereignty – steps towards a new system of internet governance*. The Fondation pour l'innovation politique.
17. European Parliament (2020), *Digital sovereignty for Europe*.
18. On 16 March 2021, the government established the Digitalisation Partnership. The Digitalisation Partnership was tasked with making recommendations to the government on how Denmark should exploit the opportunities of digitalisation in the future. Among other things, the Digitalisation Partnership has pointed out that Denmark's clear interest is to promote a vision for Europe's digital sovereignty that is open to the outside world, promote European strengths and build on collaboration with other democracies. See more at: [https://fm.dk/media/e53hnrmu/visioner-og-anbefalinger-til-danmark-som-et-digitalt-foregangsland\\_digitaliseringspartnerskabet\\_a.pdf](https://fm.dk/media/e53hnrmu/visioner-og-anbefalinger-til-danmark-som-et-digitalt-foregangsland_digitaliseringspartnerskabet_a.pdf), p. 60.
19. Adler-Nissen, R. og Eggeling, K. A. (2024), *The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X*. JCMS 2024 Vol. 62, nr. 4. p. 993-1011.
20. AWS is an American-owned company that provides cloud solutions and has data centres in Ireland, Germany, France and other countries. It is part of the Aula agreement that data must be located in a European country. See more at: <https://aulainfo.dk/guide-til-projektledere/sikkerhed-i-aula/>
21. Butler, G. (2023), *UK Home Office signs £450m cloud deal with AWS*. Located on 23 August 2024 at <https://www.datacenterdynamics.com/en/news/uk-home-office-signs-450m-cloud-deal-with-aws/>
22. DR (2024), *MitID endnu engang udsat for en type angreb, 'der kan bestilles for prisen af en caffè latte'*. Located on 23 August 2024 at <https://www.dr.dk/nyheder/indland/mitid-endnu-engang-udsat-en-type-angreb-der-kan-bestilles-prisen-af-en-caffelatte>
23. So-called electronic wallets, such as ApplePay and GooglePay, essentially function as an electronic wallet where users can place one or more cards. Payment is made with the selected payment card. Other payment solutions may work differently, for example, where payment is made account-to-account, or the customer splits the payment and is provided with credit for the purchase. See more at: <https://www.kfst.dk/media/rbdcu40/20220616-betalingsrapport-2022-final.pdf>
24. Version2 (2023), *Seks banker vil udbyde Dankort i Apple Pay – men løbet er kørt, lyder det fra betalingskæmpe*. Located on 23 August 2024 at <https://www.version2.dk/artikel/seks-banker-vil-udbyde-dankort-i-apple-pay-men-loebet-er-koert-lyder-det-fra-betalingskaempe>
25. Europa-Kommissionen (2024), *Commission seeks feedback on commitments offered by Apple over practices related to Apple Pay*. Located on 23 August 2024 at [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_282](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_282)
26. Dansk Erhverv (2024), *Langvarig kamp tager en positiv drejning: Apple frigiver afgørende betalingsteknologi*. Located on 23 August 2024 at <https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2024/februar/langvarig-kamp-tager-en-positiv-drejning-apple-frigiver-afgorende-betalingsteknologi/>
27. Digitaliseringspartnerskabet (2021), *Visioner og anbefalinger til Danmark som et digitalt foregangsland*, p. 91.
28. Find out more about DATA for GOOD at <https://dataforgoodfoundation.org/>
29. Klima-, Energi- og Forsyningsministeriet, Transportministeriet, Erhvervsministeriet og Digitaliserings- og Ligestillingsministeriet (2024), *Danmark klar til automatisering – National plan for bevægelsesdata*.
30. Dansk Erhverv (2023), *Dansk Erhverv presser på for manglende udbetalinger fra bookingselskab*. Located on 23 August 2024 at <https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2023/september/dansk-erhverv-presser-pa-for-manglende-udbetalinger-fra-bookingselskab/>
31. OpenAI (2023), *OpenAI and Microsoft extend partnership*. Located on 23 August 2024 at <https://openai.com/blog/openai-and-microsoft-extend-partnership>

32. Microsoft (2024), *Microsoft and Mistral AI announce new partnership to accelerate AI innovation and introduce Mistral Large first on Azure*. Located on 23 August 2024 at <https://azure.microsoft.com/en-us/blog/microsoft-and-mistral-ai-announce-new-partnership-to-accelerate-ai-innovation-and-introduce-mistral-large-first-on-azure/>
33. The Stack (2023), *Meta to spend up to \$33 billion on AI, as Zuckerberg pledges open approach to LLMs*. Located on 25 January 2024 at <https://www.thestack.technology/meta-ai-investment/>
34. Draghi (2024) *The future of European competitiveness*. Located on 2 November 2024 at [https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitive-ness-looking-ahead\\_en](https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitive-ness-looking-ahead_en); Letta (2024) *Much more than a market*. Located on 2 November 2024 at <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>
35. Digitaliseringspartnerskabet (2021), *Visioner og anbefalinger til Danmark som et digitalt foregangsland*, p. 102.
36. The Washington Post (2021), *Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation*. Located on 23 August 2024 at <https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/>
37. Berlingske (2024), *En løgn spredt sig med rekord fart over hele verden. Men de unge elsker TikTok og vender de gamle medier ryggen*. Located on 23 August 2024 at <https://www.berlingske.dk/kultur/en-loegn-spreder-sig-med-rekordfart-over-hele-verden-men-de-unge-elsker>
38. Mediawatch (2023), *Udenlandske selskaber tog større bid af dansk annoncemarked i 2022*. Located on 23 August 2024 at <https://mediawatch.dk/Medienyt/Kommunikation/article15698631.ece>
39. Radar (2024), *Få overblikket: Sådan er kommunerne fanget i Microsofts systemer*. Located on 23 August 2024 at <https://radar.dk/artikel/faa-overblikket-saadan-er-kommunerne-fanget-i-microsofts-systemer>
40. Center for Cybersikkerhed (2023), *CFCS' anbefaling vedrørende TikTok*. Located on 23 August 2024 at <https://www.cfcs.dk/da/nyheder/2023/cfcs-anbefaling-tiktok/>
41. IT-Branchen (2023), *Fremtidens beskyttelse af det digitale Danmark*.
42. See for example. Version2 (2016), *It-firma om offentligt kæmpe-udbud til skoler og børnehaver: De skaber et monopol*. Located on 23 August 2024 at <https://www.version2.dk/artikel/it-firma-om-offentligt-kaempe-udbud-til-skoler-og-boernehaver-de-skaber-et-monopol>
43. Børne- og Undervisningsministeriet (2021), *Ny kortlægning: En velfungerende digital hverdag med plads til forbedring*. Located on 23 August 2024 at <https://www.uvm.dk/aktuelt/nyheder/uvmm/2021/maj/210517-ny-kortlaegning-en-velfungerende-digital-hverdag-med-plads-til-forbedring>
44. Christensen, Beuchert og Rasmussen (2022), *PISA 2022: Hovedrapport, VIVE – Det Nationale Forsknings- og Analysecenter for Velfærd*.
45. Cone og Lai (2024), *A day in the (datafied) life: Digital education platforms, commercial infrastructures, and the (im)possibilities of disconnection*, i *The Digital Backlash and the Paradoxes of Disconnection* / [ed] K. Albris, K. Fast, F. Karlsen, A. Kaun, S. Lomborg, & T. Syvertsen, Nordicom, Located on 2 November 2024 at <https://norden.diva-portal.org/smash/record.jsf?pid=diva2%3A1896989&dsid=-1403>
46. Version2 (2024), *Googles skole-software koster det samme som en cheeseburger: Ekspertes er ikke i tvivl om hvorfor*. Located on 23 August 2024 at <https://www.version2.dk/artikel/googles-skole-software-koster-det-samme-som-en-cheeseburger-ekspertes-er-ikke-i-tvivl-om-hvorfor>
47. DR (2024), *Danske forældre på jagt efter børnesandaler snydt af falske webshops*. Located on 23 August 2024 at <https://www.dr.dk/nyheder/indland/danske-foraeldre-paa-jagt-efter-boernesandaler-snydt-af-falske-webshops>





Regeringens ekspertgruppe

---

**TECH-GIGANTER**