

THE DANISH
INSTITUTE FOR
HUMAN RIGHTS

TECH GIANTS,
FREEDOM OF
EXPRESSION AND
PRIVACY



TECH GIANTS, FREEDOM OF EXPRESSION AND PRIVACY

Rikke Frank Jørgensen & Marya Akhtar

e-ISBN: 978-87-93893-77-1

© 2020 The Danish Institute for Human Rights
Wilders Plads 8K
DK-1403 Copenhagen K
Phone +45 3269 8888
www.humanrights.dk

Provided such reproduction is for non-commercial use, this publication, or parts of it, may be reproduced if author and source are quoted.

At DIHR we aim to make our publications as accessible as possible. We use large font size, short (hyphen-free) lines, left-aligned text and strong contrast for maximum legibility. For further information about accessibility please click www.humanrights.dk/accessibility

CONTENT

1 EXECUTIVE SUMMARY	5
2 INTRODUCTION	7
3 WHAT IS A TECH GIANT	9
4 HUMAN RIGHTS PROTECTION	11
4.1 THE UN	11
4.1.1 binding rules	11
4.1.2 guidelines and recommendations	13
4.2 THE COUNCIL OF EUROPE AND THE EUROPEAN COURT OF HUMAN RIGHT	14
4.2.1 binding rules	14
4.2.1.1 Freedom of expression and information	15
4.2.1.2 Privacy and personal data	16
4.2.2 guidelines and recommendations	18
4.3 THE EU	18
4.3.1 binding rules	18
4.3.1.1 Freedom of expression and information	19
4.3.1.2 Privacy and personal data	21
4.3.2 guidelines and recommendations	24
4.4 DANISH LAW	25
5 TECH GIANTS AND HUMAN RIGHTS CHALLENGES	ERROR! BOOKMARK NOT DEFINED.
5.1 FREEDOM OF EXPRESSION AND INFORMATION	27
5.1.1 legal content, illegal content and grey areas	27
5.1.1.1 Legal basis requirement	29
5.1.1.2 GNI.....	29
5.1.2 challenges in access to effective remedies	34
5.1.3 risks of using automated content filters	36
5.1.3.1 Automated content filters.....	36
5.1.3.2 <i>Upload</i> filters.....	37
5.1.3.3 Automated selection of content	38
5.2 THE RIGHT TO RESPECT FOR PRIVATE LIFE AND THE PROTECTION OF PERSONAL DATA	40
5.2.1 surveillance capitalism	40
5.2.1.1 Lack of transparency	42
5.2.1.2 Competition law as human rights protection	43
5.2.1.3 Increased risks due to automisation	44
5.2.2 Data protection challenges related to tech giant practice	45

5.2.2.1 Data minimisation	46
5.2.2.2 Purpose limitation	47
5.2.2.3 Right of access	47
5.2.2.4 Consent	48
5.2.2.5 Lack of review by the European Courts	49
6 SELECTED PUBLICATIONS FROM THE DANISH INSTITUTE FOR HUMAN RIGHTS.....	50
6.1 FACT SHEETS	50
6.2 REPORTS	50
6.3 CONSULTATION RESPONSES	51
6.4 PUBLICATIONS.....	51

1 EXECUTIVE SUMMARY

Tech giants are playing an **ever-increasing role in society**, because they control the platforms and services on which communication, search for information, public debate, etc. plays out. At the same time, these companies operate (to varying extents) with a business model based on collecting and analysing as much information on users as possible.

So far, tech giants have had unprecedented opportunity to impact human rights and democratic processes for millions of people, while acting outside democratic control.

The companies thus have significant influence on the rights of the individual, while at the same time operating in a **regulatory void** in several areas. It has been up to the companies themselves to ensure that they respect human rights law.

This report describes human rights issues raised by tech giants with special focus on:

- **Freedom of expression**, including the grey zones that currently exist for protecting freedom of expression on digital platforms.
- **The right to privacy and protection of personal data**, including the collection and commercial use of this data by platforms.
- **Effective enforcement** of human rights.

Tech giants remove content from the internet for many different reasons. For example, content may be removed because a state has specifically ordered the platform to remove the content, or because the platform itself has decided that certain types of content should not be visible on their platforms. Content may also be removed because the state has encouraged the company to do so, or because the platform has entered into a voluntary agreement with the state to remove the content. Considering the variety of reasons why content may be removed, **the state's responsibility to protect freedom of expression is rather unclear**.

In practice, tech giants are expected to assess large volumes of content in order to remove illegal content. This creates a risk of **over-regulation**, so that more

content than necessary is removed. Over-regulation of content can lead to a *chilling effect* on freedom of expression and information.

Concerns over having private actors assess whether content is illegal are accentuated when this assessment is conducted via **automated content filters**.

Extensive collection and use of personal data by tech giants has been referred to as **surveillance capitalism**. **Surveillance capitalism has created new products and markets** based on the possibility to predict and influence people's behaviour.

The current market structure means that data on individuals is being shared and used by many actors that the individual does not know about. The non-transparent relationships between actors mean that **people do not know to whom they should direct any complaints**.

The non-transparent interplay between the many actors on the market leads to a **loss of rights**. The business model also challenges several core data protection law principles: requirements for **data minimisation, purpose limitation, (informed) consent and access**.

2 INTRODUCTION

Tech giants such as Google, Apple, Amazon, Microsoft and Facebook have wide discretion to define terms and conditions for the use of their services because they are private companies. As their **role in society is becoming more dominant**, there is increasing attention to how their platforms and services interfere with the democratic life of society and with human rights.

The purpose of this report is to provide an overview of the **human rights issues** that arise when tech giants assume an ever-more dominant role in society. The report focuses on two key rights: **freedom of expression and information as well as the right to respect for private life**.

Freedom of expression is generally impacted by tech giants in two types of situations:

1. States use regulation to impose upon companies the responsibility to **remove illegal content**, thus **interfering with freedom of expression**.
2. Companies themselves implement content regulation that restricts **legal content**.

The role of tech giants also challenges privacy and the protection of personal data, as collection, analysis and sharing of large amounts of user data form the basis for new types of surveillance and control by both states and companies.¹

However, **other rights** can also be affected, but these are not addressed in this report. For instance, the UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association has stressed that the conduct of companies also affects the freedom of association.² Moreover, questions have been raised as to whether targeted advertisements, including housing and job advertisements, conflict with the prohibition of discrimination.³ More generally, the question of the role of tech giants in democracy has been subject to debate, among other things in relation to the question of disinformation, political campaigns and the tone on social media.⁴

The rest of the report is structured as follows: **Section 3** explains the term "tech giant", and **section 4** reviews the right to freedom of expression and information as well as the right to privacy. **Section 5** highlights the most important human

rights issues regarding the relationship between states, companies and individuals.

CHAPTER 3

WHAT IS A TECH GIANT?

Tech giant is not a legal term. However, it is used to describe technology companies that have obtained a dominant position on the market through the spread of their platforms and services.

With the development of digital society, tech giants have been the subject of increasing attention as they increasingly control the platforms and services on which communication, information search, public debate, etc. play out. Influence on the possibilities of individuals to exercise their human rights has thus concentrated around these relatively few companies.

In a European context, Apple, Amazon, Google, Facebook and Microsoft are usually referred to as tech giants. These companies offer a number of services and platforms within a wide-ranging set of activities such as marketplaces, search engines, social media, application distribution platforms, payment systems, and platforms for the collaborative economy.⁵

This report uses tech giants as a generic term for technology companies whose size and position on the market push specific human rights issues to the forefront.

Some of the rights particularly affected are freedom of expression and freedom of information, the right to privacy, and the protection of personal data. For example, the companies decide which conversations they will allow, which content they will remove, which information is presented to the individual user, and how they use the large amounts of data they collect on each user of the platform.⁶

The companies' business model is based on collection, analysis, and use of data, including personal data on users of the platform. This data is used commercially by the companies and is also exchanged with states, for example for investigation and intelligence activities.

In this context, a significant feature of the digital era is that the infrastructures for freedom of expression and freedom of information have merged with infrastructures for public and private surveillance within the same few and large companies.⁷ **The channels on which users depend to communicate are the same as those the state (and companies) use to surveil users.**

Tech giants have unique commercial power and innovation strength on the market, while influencing democracy and exchanges of views and creating detailed profiles of users.⁸

This development means that tech giants have an unprecedented opportunity to impact human rights and democratic processes for millions of people, while acting beyond democratic control. The companies' control of digital platforms and services also means that states must go through tech giants when they want to control content on the internet, for example when states want unlawful expressions to be removed.

This special position in society is referred to as a "**gatekeeper**".⁹ Due to their special position on the market, the companies exert considerable control over access to a key resource for society. A gatekeeper position raises questions about the legal and/or social **obligations** of the companies in society due to their market position, status and/or influence on democracy.¹⁰ For example, one important aspect is whether the user has other similar options to participate in the public debate.

It has been emphasised that tech giants possess **a new type of power** in terms of communicating news, enabling democratic processes and collective action as well as information search and communicating views, including opinions that dissent from those in power.¹¹

It has been said that the platforms and services of tech giants have become fundamental to the modern world and to how people interact with each other.¹²

This dominant role in society makes it essential to ensure that the rights of individuals are protected on the platforms on which the rights play out. This report shows that this is not the case today.

CHAPTER 4

HUMAN RIGHTS PROTECTION

Human rights bind the states that have signed the international conventions, whereas companies are not **obligated directly** by human rights law, because they are private actors.

A state is obligated to protect the individual against violations from companies (this is referred to as **positive obligation**). The scope of a state's positive obligations depends on the specific circumstances (see section 4.2.1 below). If a state chooses to regulate the conduct of companies, the companies must comply with the regulations laid down, and in doing so they **indirectly become subject to** human rights law.

EU law can bind private actors directly to comply with certain rights. For example, both private and public actors are obligated to protect personal data according to the General Data Protection Regulation (see section 4.3.1 below).

The following provides an overview of the most important human rights sources to assess the conduct of tech giants.

4.1 THE UN

4.1.1 BINDING RULES

The UN International Covenant on Civil and Political Rights protects the freedom of expression and information (Article 19) and the right to respect for private life (Article 17). The provisions obligate states to respect these rights. However, the provisions are not aimed at private companies, and tech giants are therefore *not* covered.

The right to privacy is closely linked to other freedoms such as freedom of expression, and **the full effects of both these rights are mutually entwined.**¹³

A state can interfere with freedom of expression and information as well as the right to respect for private life. For an interference to be compatible with human

rights law, it must be prescribed by law, pursue a legitimate aim and be necessary (including proportionality). A state can thus regulate freedom of expression and interference with private life.

The Danish Institute for Human Rights has prepared an overview of human rights protection of private life and data protection [here](#). See also section 4.2.1 for a more detailed review of the two rights.

In special cases, **the state has a human rights obligation to curtail** freedom of expression and criminalise expressions in order to prevent violence, hatred and assault. It therefore follows from Article 20(2) of the Covenant that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law. According to Article 26, the state is also obligated to guarantee to all people an effective protection against discrimination. As part of this protection, many states have adopted legislation targeted at hate speech.

According to Articles 4 and 5 of the **UN International Convention on the Elimination of All Forms of Racial Discrimination**, states are also committed to taking measures to combat any incitement to, or acts of, racial discrimination. States must declare as an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any persons of another ethnic origin.

The relationship between Articles 19 and 20 of the International Covenant on Civil and Political Rights and Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination was most recently addressed by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, who stressed that the two types of rights require interpretation and specific guidance.¹⁴

The Committee on the Elimination of Racial Discrimination has stated that criminalisation of racist expression according to Article 4 should be reserved for serious cases.¹⁵

See also the Danish Institute for Human Rights report on hate speech in the public debate, which contains a review of human rights regulation of hate speech. The report is available [here](#).

4.1.2 GUIDELINES AND RECOMMENDATIONS

In 2011, the UN adopted a set of Guiding Principles **on Business and Human Rights** that include state obligations as well as corporate responsibility.¹⁶ **The Guiding Principles are not binding** but assume that companies themselves will take steps to organise their business so that they respect human rights.

The Guiding Principles represent a global standard of expected conduct for all companies. Among other things, companies are expected to demonstrate human rights due diligence as an integrated part of their business, and to carry out human rights impact assessments.¹⁷

FACEBOOK IN MYANMAR

An example of a human rights impact assessment is the Facebook assessment of Myanmar and the role of Facebook in the spread of hate speech.¹⁸ In 2014, Facebook expanded to Myanmar, and over three years the number of Facebook users grew from 2 to 30 million.¹⁹ In parallel, the conflict between the Rohingya minority and the Myanmar military escalated, and this led to extensive ethnic cleansing of the Rohingya. According to a UN report, Facebook was a useful instrument for those seeking to spread hate in the country.²⁰ Messages and comments which should have been removed according to Facebook's own guidelines were in many cases not removed, partly because Facebook did not have enough employees who knew the Myanmar language.

In 2012, the UN established for the first time that human rights should apply **online** as well as **offline**. Since then the relationship between technology and human rights has been addressed in several non-binding standards and recommendations.

For an overview of the UN standards for the area, see the Danish Institute for Human Rights fact sheet [here](#).

In recent years, several UN special rapporteurs have focused on the conduct of tech giants.

In a report from 2018, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression identified two key challenges with regard to regulation of content on social media etc. The first challenge is that **states are increasingly adopting legislation that restricts people's freedom of expression on digital platforms**, including by putting pressure on companies to restrict certain types of content. The other challenge is that **content regulation by companies lacks transparency and consistency**. With regard to the latter, the Special Rapporteur takes outset in the UN Guiding Principles on Business and Human Rights.²¹

The UN Special Rapporteur on the Right to Privacy also stressed the human rights challenges of the digital era on the basis of the UN Guiding Principles. Among other things, the Rapporteur recommends that companies should fully adopt the UN Guiding Principles in their business, ensure a high level of security and confidentiality in people's communication, and ensure the greatest possible transparency in the internal policies and practices that implicate the right to privacy of users.²²

4.2 THE COUNCIL OF EUROPE AND THE EUROPEAN COURT OF HUMAN RIGHT

4.2.1 BINDING RULES

(Article 10) **and the right to respect for private life** (Article 8). As mentioned in section 4.1.1, restrictions on freedom of expression and private life must be prescribed by law, pursue a legitimate aim and be necessary (including proportionality).

Article 13 of the Convention entails that everyone whose rights are violated must have an effective remedy before a national authority, notwithstanding that the violation has been committed by the state or private individuals.

The Council of Europe Convention on Cybercrime from 2001 and the Additional Protocol from 2003 govern hate speech motivated by racism and xenophobia.

The Additional Protocol requires member states to criminalise online expressions of a racist or xenophobic nature.

4.2.1.1 Freedom of expression and information

Freedom of expression and information includes freedom to hold and express opinions as well as to seek, receive, impart and access information. Freedom of expression not only covers words, but also images and sound.

The European Court of Human Rights has not explicitly considered the significance of tech giants for freedom of expression (or other human rights). However, the Court has stated more generally that access to the internet plays a major role for public access to information, debate, news and the dissemination of information otherwise.²³

In **Delfi AS v. Estonia**, the European Court of Human Rights decided for the first time on a platform's responsibility to remove illegal content. The case dealt with hate speech on a news portal (Delfi), and whether Delfi had removed a defamatory comment quickly enough. The Court assessed that Delfi had *failed* to act expeditiously to remove the illegal content after they had become aware of this, and that imposing on Delfi a responsibility to act expeditiously was *not* a violation of the freedom of expression. The Court stressed in its decision that Delfi had a commercial interest in sharing content generated by users, and that Delfi was the largest news platform in Estonia and not a social medium.²⁴ A closer examination of the ruling is available in the Danish Institute for Human Rights EU study on ICT and human rights (FRAME) [here](#).

In its practice, the European Court of Human Rights has stated that a state's obligation to respect Article 10 also includes certain **positive obligations**. The scope of a state's positive obligations involves an assessment of the kind of rights

of expression at stake, their capability to contribute to public debates, the nature and scope of restrictions on the rights, alternative venues for expression, and the impact of the expressions on other rights.²⁵

Restrictions on freedom of expression

In some cases, the protection in Article 8 and Article 10 may conflict. This may be in connection with balancing the two rights in relation to images, expressions, or information concerning private matters. In this regard, the Court has ruled that states have a broad margin of appreciation in enforcing the two rights when they conflict with each other.²⁶ In some cases, protection of private life according to Article 8 can lead to restrictions on the right to freedom of expression according to Article 10.

For instance, regarding Article 8, the Court has pointed out that a state's positive obligation entails that the state launch investigations following reasonably justified allegations of violation.²⁷ Among other things, this duty entails that the state ensure effective remedies to allow identification and prosecution of people who violate others on the internet.²⁸

According to Article 8, the state also has a positive obligation to protect the individual against degrading and insulting expressions about a group of persons on grounds such as race, religion or sexual orientation.²⁹

Abusive or offensive expressions intended to undermine the purpose of the Convention will not be protected by the Convention according to Article 17 on abuse of rights. For example, Article 17 is used for expressions that incite or encourage terrorism, hatred, killings or crimes against the sovereignty and security of the state.³⁰

4.2.1.2 Privacy and personal data

The right to respect for private life stipulates that no one may be subjected to arbitrary interference with his privacy, family, home or correspondence. This right to privacy also includes certain information (personal data) on the individual.³¹ Everyone has the right to the protection of the law against such interference.

The European Court of Human Rights has established that the protection of personal data also entails a right to self-determination with regard to own personal data:

"The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life [...]. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged."³²

In addition, the Court has stated that use of information for purposes other than those for which the information was originally obtained is restricted by the protection in Article 8.³³

Moreover, the Court has stated that the fact that subsequent use of the information may be legal does not at all exempt from the requirement of legal authority to collect the information. The Court made a statement about this in a case regarding video recorded by the police without legal authority. The recordings were subsequently used during a trial. In this regard, the Court stated that:

"Issues relating to the fairness of the use of the evidence in the trial must [...] be distinguished from the question of lawfulness of the interference with private life and are relevant rather to Article 6 than to Article 8."³⁴

The question about authorities' access to information on the internet, including mass surveillance, is currently being examined in two pending cases by the Court's Grand Chamber.³⁵

In addition to Article 8 of the European Convention on Human Rights, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) and the amending Protocol (2018) apply, ensuring the right to privacy in connection with processing of personal data.³⁶

4.2.2 GUIDELINES AND RECOMMENDATIONS

The Council of Europe has adopted a series of **declarations and recommendations** on the relationship between technology and human rights, including with regard to social media, search engines, artificial intelligence, algorithms, Big Data, surveillance and the rights of internet users. These standards are normative, but not legally binding.

Among other things, in its recommendation regarding freedom of expression and internet filters, the Committee of Ministers of the Council of Europe states that member states are obligated to ensure freedom of expression in their regulation of the use of internet filters.³⁷ Similarly, in 2016 the Committee of Ministers adopted the first recommendation regarding human rights and business, which builds on the UN Guiding Principles and encourages member states of the Council of Europe to enhance national implementation of these principles.³⁸

The Parliamentary Assembly of the Council of Europe has also adopted a number of standards concerning technology and human rights, including Resolution 1843 (2011) on the protection of privacy and personal data on the internet and online media³⁹ and Resolution 2311 on human rights and business.⁴⁰

The Danish Institute for Human Rights has drawn up a fact sheet of the standards of the Council of Europe within human rights and technology. The fact sheet is available [here](#).⁴¹

4.3 THE EU

4.3.1 BINDING RULES

The Charter of Fundamental Rights of the European Union protects **freedom of expression and information** (Article 11) and **the right to respect for private life** (Article 7) as well as **processing of personal data** (Article 8).⁴²

Article 47 of the Charter states that everyone whose rights and freedoms are violated has the right to an effective remedy before a tribunal.

4.3.1.1 Freedom of expression and information

Like the UN International Covenant on Civil and Political Rights and the European Convention on Human Rights, Article 11 of the Charter regarding freedom of expression only binds states, and this is clear from the wording of the provision.

On the other hand, there are **binding rules in the EU that obligate private actors to remove illegal content from their platforms and these rules can constitute interference with the freedom of expression and information**. This is because, in these situations, companies act on the basis of an obligation laid down by the member states or the EU.

It follows from the **Directive on electronic commerce**,⁴³ that providers of digital services are in principle exempted from liability for the content they disseminate, but that they are obligated to remove illegal content when they obtain knowledge or awareness of it (Article 14). If the company fails to do so, it may be held liable for complicity in the illegal activity. This special form of "duty to act" is referred to as the **notice and takedown principle**.⁴⁴

Moreover, Article 15 of the Directive states that member states **must not impose a general obligation on companies to monitor** the content on their services and platforms. **Thus, the relationship between restrictions on freedom of expression and monitoring is explicit in the Directive on electronic commerce.**

Section 5.2 below addresses filtering and review of content on the internet by companies in relation to privacy.

For a more detailed description of the impact of the Directive on electronic commerce on social media practice, see the Danish Institute for Human Rights report on democratic participation on Facebook. Among other things, the report concludes that there is a need to specify social media's "duty to act" according to the Directive on electronic commerce as well as effective enforcement of social media's complicity liability if they fail to remove illegal content in due time. The report is available [here](#).

The Directive on electronic commerce is currently being revised by the EU, and the scene has been set for a wide-ranging reform of the liability of platforms.⁴⁵

Obligations to remove content aimed at platforms and other private actors on the internet also follow from other EU law, including: the Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography⁴⁶, the Directive on Copyright and Related Rights in the Digital Single Market⁴⁷, and the amending Directive on Audiovisual Media Services.⁴⁸ See the Danish Institute for Human Rights consultation response on the amending Directive and its Danish implementation [here](#).

Most recently, the EU is negotiating a regulation to prevent the dissemination of **terrorist content online**, which contains a number of obligations for companies to remove illegal content. The Danish Institute for Human Rights has taken a position on previous versions of the draft regulation [here](#) and [here](#).

The European Court of Justice has looked closer at the obligations of digital platforms and services in a number of judgments.

In **SABAM v. Scarlet Extended**⁴⁹, the Court ruled on the issue of use of content filtering to prevent infringement of intellectual property rights.⁵⁰ The Court found that companies may not be required to use a content filter, as this corresponds to temporally unlimited monitoring of all information on users. Such general monitoring conflicts with Article 15 of the Directive on electronic commerce. The Court stressed that the use of filters can infringe on the protection of personal data in **Article 8 of the Charter** and the freedom to receive and impart information in **Article 11 of the Charter**.⁵¹

Most recently, the European Court of Justice decided in **Glawischnig-Piesczek v. Facebook Ireland Limited** that Article 15 of the Directive on electronic commerce does not prevent a member state from ordering Facebook to remove illegal content. This also includes "information with an equivalent meaning", previously declared to be illegal. However, the Court stressed that the order must not require Facebook to carry out "an independent assessment" of the content.⁵³ The Court did not specify what constitutes an "independent assessment", but stated that the platform must use "automated search tools and technologies".⁵⁴ The judgment provides no answer as to how quickly and effectively Facebook or other platforms must remove illegal user-generated content.

Use of automated methods (content filters etc.) raises some important human rights issues dealt with in more detail in section 5.1.2 below. The Court did not consider these issues in its judgment.

4.3.1.2 Privacy and personal data

The right to respect for private life is protected in Article 7 of the Charter. The Charter also explicitly protects personal data in Article 8.

Within EU law, certain human rights have a **direct impact between private individuals**. For example, this applies to the right to data protection implemented in the **General Data Protection Regulation**.⁵⁵

Articles 6 and 9 regulate processing of personal data by both public and private actors. In the case of collection of information about individuals by the platforms, the clear basis is that **consent** must be given to companies before they can collect and use personal data. Personal data is to be understood in a broad sense as any information that can be related to a person, see Article 4.⁵⁶

The Regulation builds on a number of key principles for protection of personal data, including in particular: the **principle of lawfulness, fairness and transparency** in connection with processing of personal data, see Article 5(1)a of the Regulation, **purpose limitation** (Article 5(1)b), according to which personal data may not be used for purposes that are incompatible with the **purposes** for which it was collected, as well as the principle of **data minimisation** (Article 5(1)c), according to which no more personal data than is strictly necessary must be collected.

The Regulation also grants individuals a set of rights in relation to the company, including in particular: the **right of access and right to object** in connection with collected personal data, for example, the right to object to disclosure of data for **marketing purposes** (Article 21(2)), the right to **rectification of data** (Article 16), the right to erasure of data, also referred to as the **right to be forgotten** (Article 17) as well as the right to **data portability** (Article 20).

The General Data Protection Regulation entered into force in May 2018. Its future interpretation, including in relation to collection and use of personal data by companies, will be stipulated by the European Court of Justice as cases are ruled in the area. In Denmark, the Regulation is supplemented by the Data Protection Act.⁵⁷

In addition to the General Data Protection Regulation, the Directive concerning data protection within electronic communications (**the eData Protection Directive, also referred to as the ePrivacy Directive**)⁵⁸ also applies. Among other things, this directive regulates storage of traffic data for electronic communication. The e-Data Protection Directive is currently being revised and is expected to be replaced by a regulation to modernise the rules and to adapt and add these rules to the General Data Protection Regulation and bring them in line with the digital reality, including by increasing regulation of tech giant communication services.⁵⁹

The current e-Data Protection Directive is key in the legal practice of logging developed by the European Court of Justice.⁶⁰

The Directive was also applied by the European Court of Justice in **Planet49**⁶¹ with regard to the duty of companies to obtain active consent to store cookies.

A number of the fundamental principles and rules in the General Data Protection Regulation and the e-Data Protection Directive have long been the applicable law in the EU, and the Court has had reason to develop them and relate to them.

In its legal practice, the European Court of Justice has looked at **the right to be forgotten** (by having links to websites with personal data removed from Google's search index) **in relation to the protection of freedom of expression.**

In **Google Spain**⁶², the Court found that, under certain conditions, an EU citizen is entitled to have links to websites removed that contain information relating to that person which is **no longer relevant** (the right to be forgotten). Among other things, the Court emphasised that search engines enable interconnection of information, by which a more or less detailed profile can be established of the person.⁶³ The Court established that a search engine may be obligated to remove

links from its search index, even when these links refer to websites on which this information is lawful.⁶⁴

Most recently, in **CNIL v. Google**⁶⁵, the European Court of Justice stated that the previous ruling does not entail an obligation for Google to remove links for citizens outside the EU. The Court of Justice emphasised that the right to **protection of personal data is not an absolute right, but** it must be balanced against other fundamental rights. The balance between the right to respect for private life and the protection of personal data and the freedom of information **will in practice vary significantly around the world.**⁶⁶ Also within the EU, it is possible that a specific balancing of the two rights could lead to varying results from one country to another.⁶⁷

In other cases, the European Court of Justice has considered the question of jurisdiction, which can create specific difficulties in relation to tech giants that are often established outside the EU.

In **Wirtschaftsakademie**⁶⁸, the Court found that Facebook's office in Germany was covered by the jurisdiction of the German data protection authority, even though the office was only responsible for selling advertising space. In this specific case, the Court assessed that Facebook Germany was the data controller together with a German company that had set up a fan page on Facebook. As Facebook collected information from the fan page for targeted advertising aimed at German citizens, the German data protection authority could set requirements for the processing of personal data.⁶⁹

The European Court of Justice has also examined **sharing of personal data to foreign authorities via Facebook.**

One of the most significant judgments in this area is **Maximillian Schrems**,⁷⁰ which is about the so-called "**safe harbour agreement**"⁷¹ between the European Commission and the US. According to the agreement, personal data on EU citizens could be disclosed to other countries that had an "adequate level of protection" for the data. The case concerned Facebook's transfer of data on EU citizens to the US and resulted in the "safe harbour agreement" being overruled. The Court emphasised that the European Commission had **limited discretion** to

assess whether the US level of protection was adequate, and that they had to conduct a **strict review** of the requirements that followed from EU law regarding personal data and privacy before transfer to the US could be allowed.⁷² The Court did *not* find that the "safe harbour agreement" met these requirements and emphasised, among other things, that the scheme was superseded by US security requirements, and therefore personal data of EU citizens was not protected against interference from US authorities. Nor was there any effective judicial protection against such interference.

The "*safe harbour*" scheme was subsequently replaced by the "**privacy shield agreement**", the lawfulness of which is currently being reviewed by the European Court of Justice.⁷³

The Court has also addressed who should be considered the data controller when data is collected and shared between several companies for commercial purposes.

The case of **Fashion ID**⁷⁴ concerned a company's use of the Facebook "Like" button on its website. Use of the button meant that data on users of Fashion ID's website was shared with Facebook. The Court concluded that Fashion ID and Facebook were **jointly responsible** for the personal data.⁷⁵ With regard to requirements for **consent** and **duty to inform** in relation to the user, Fashion ID and not Facebook had to ensure compliance with rules, as requirements for consent and information must be fulfilled *prior* to the collection of personal data.⁷⁶ In this case, the European Court of Justice found that a pre-ticked field does *not* constitute valid consent, as this requires active action from the user.

4.3.2 GUIDELINES AND RECOMMENDATIONS

A number of guidelines and recommendations concerning tech giants have also been adopted within the EU.

Some of the most important examples include the **Code of Conduct** between the European Commission and Facebook, Microsoft, Twitter and YouTube on countering hate speech⁷⁷ as well as ongoing work regarding the responsibilities and duties of digital platforms.⁷⁸

In this connection, the Commission Recommendation on measures to effectively tackle illegal content online is key, as it elaborates on some of the initiatives that the European Commission urges the companies to launch in order to tackle illegal content.⁷⁹

For a more detailed description of issues regarding EU law linked to regulation of content and freedom of expression, see the Danish Institute for Human Rights EU study on ICT and human rights (FRAME) [here](#).

See also the institute's factsheet on content filters and the platforms' regulation of freedom of expression [here](#).

Within protection of privacy and personal data, a number of statements from the former Article 29 Working Party and the current European Data Protection Board contribute to interpretation of the scope of the protection.

4.4 DANISH LAW

Protection of freedom of expression follows from section **77 of the Constitutional Act of Denmark** and is directed towards the state.

The issue of social media and freedom of expression has also been examined by the Freedom of Expression Commission set up by the Danish Ministry of Justice, and the Commission's report was published in April 2020.⁸⁰ The Danish government has expressed that it awaits the Commission's analysis before introducing any Danish regulation in the area.⁸¹

Danish rules on criminal and tort liability for complicity may mean that providers of digital platforms and services can be held liable for illegal content online.

Within criminal law, this may be liability for complicity for digital sexual offences,⁸² defamation according to the Danish Penal Code or violations of the section on racism in the Danish Penal Code.

The Danish Institute for Human Rights has previously [stressed](#) a need to clarify the frameworks for liability for complicity, for example how quickly a platform is expected to react.

With regard to **protection of personal data**, in Denmark the General Data Protection Regulation is supplemented by the Data Protection Act, and the Danish Data Protection Agency monitors both sets of regulations and issues guidelines etc. for the area.

CHAPTER 5

TECH GIANTS AND HUMAN RIGHTS CHALLENGES

5.1 FREEDOM OF EXPRESSION AND INFORMATION

5.1.1 LEGAL CONTENT, ILLEGAL CONTENT AND GREY AREAS

In order to understand the impact of companies on people's freedom of expression and information, it is important to **distinguish between legal and illegal content**.

Freedom of expression is not an absolute right, but its limits are defined in laws to prevent arbitrary interference. In brief, this means that expressions that are not prohibited by law are allowed. Furthermore, the legal basis is that anyone who makes an expression is responsible for this expression.

At the same time, a state must ensure compliance with **other human rights obligations**, such as Article 8 of the European Convention on Human Rights, Article 20(2) of the International Covenant on Civil and Political Rights and Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination. Therein lies a need for quick reaction when illegal content is identified, so that the content is not available and is not shared any further.

When companies remove **illegal content** according to a **specific order from a state, the state** must ensure that freedom of expression is not violated. In such situations, the company will **enforce** the order from the state, and the human rights responsibility is clear.

However, if this is not a specific order, but rather a **general obligation pursuant to legislation**, the situation is moving towards a grey area in terms of the responsibility of the state.

For example, companies are subject to a *notice and takedown* obligation according to the Directive on electronic commerce. This could be referred to as a general obligation pursuant to legislation.

If there are no general obligations in legislation to remove content, but rather **requests or recommendations** from the state to companies, the question of the human rights responsibility is even more unclear: is the state still responsible for ensuring that freedom of expression is not violated in situations in which the company removes content?

This also applies when a state enters into **voluntary agreements** with the platforms or issues non-binding guidelines on regulation of content.

There are also situations in which companies' own **terms and conditions** in practice lead to the removal of large quantities of **legal content**. All the large platforms have their own terms and conditions stipulating which topics can be debated, regardless of whether the content is legal. Moreover, companies select which content the user is presented with or can access. Regulation of legal content by platforms is based on the standards for acceptable expressions and good conduct defined by the individual platform. These are **commercially defined restrictions** as opposed to restrictions based on human rights standards for freedom of expression.



The many grey areas mean that tech giants operate without clear legal rules, and this is particularly problematic in terms of their massive impact on society and democracy. Because the grey areas are not legally clear, there is a risk that companies remove legal content to be "on the safe side". The risk of over-regulation has led to recommendations that **a state should always impose obligations on companies through legislation.**⁸³

5.1.1.1 Legal basis requirement

Human rights law imposes requirements on states stipulating that interference with freedom of expression must be **warranted**. This requirement sets certain conditions for the legal basis, as a legal basis must be defined with sufficient clarity and precision, and it must be available to citizens. The objective is for people to be able to adjust their conduct and be able to predict the consequences of any action or expression.⁸⁴

The human rights legal basis requirement is challenged by the grey areas above (section 5.1.1). For example, the legal basis requirement is unlikely to be met by voluntary agreements between the state and the platforms.⁸⁵ Moreover, the legal basis requirement will raise questions about how precise a general obligation on notice and takedown is to be to meet the requirement.

5.1.1.2 GNI

For many years, tech giants have focused on requests from states to remove content and/or provide data on their users. In 2008, the tech giants set up their own industry network, the **Global Network Initiative (GNI)**, which has developed guidelines for how companies can respect the freedom of expression and privacy rights of their users when dealing with requests from states. As part of this work, many companies publish annual transparency reports, in which they document the number of requests from states they have received and granted. However, there are no statutory requirements for these transparency reports, and coordination of companies' removal of content via GNI has been criticised for lacking transparency.⁸⁶

The current practice of tech giants is mainly such that state requests (concerning illegal content) are dealt with on the basis of human rights standards for legal authority, legitimate aim and necessity (including proportionality), whereas companies' own processes (concerning legal content) – for example their enforcement of so-called community standards – are not considered a human rights issue.⁸⁷

All this leads to **three unclarified issues** for the protection of freedom of expression:

1. How far-reaching should the state's responsibility to ensure freedom of expression be in the **grey areas** between specific orders to remove **illegal content** and companies' removal of **legal content** according to their own terms and conditions?
2. Should tech giants be ordered to **protect the freedom of expression in their terms and conditions when removing legal content**, and if so, how far should their responsibilities extend?
3. Should the state, as part of its positive obligation to ensure the freedom of expression, **regulate the practice of tech giants regarding legal content**?

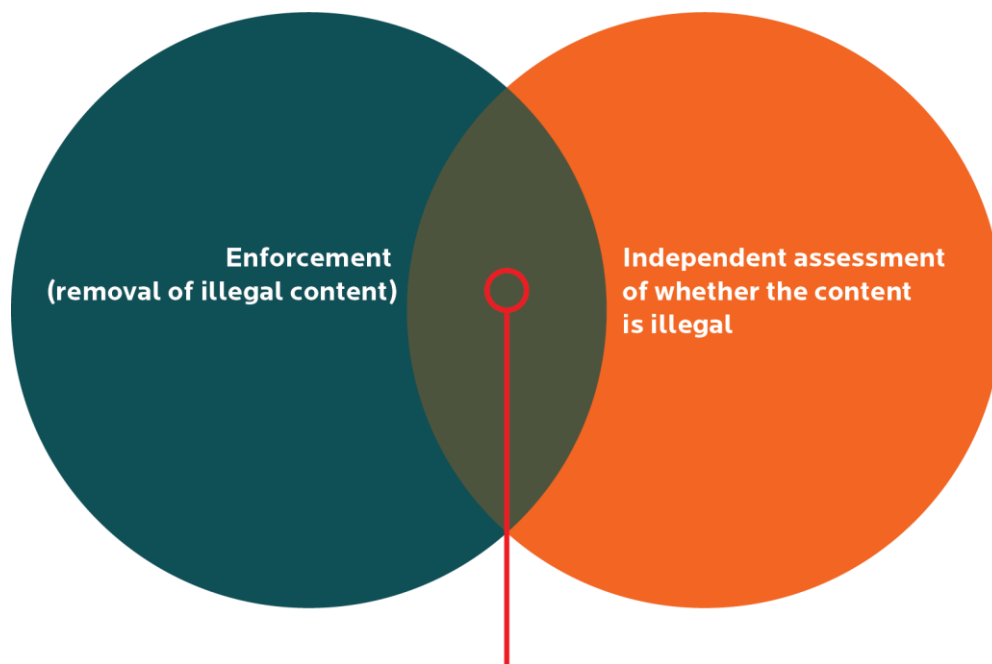
Questions 1 is about the state's responsibility regarding all digital platforms and services, etc., and not only tech giants. However, the size and market dominance of the company as well as its importance to society and democracy will affect the consequences of the interference.

Determining whether the content is illegal will often be a complex legal assessment which may include many conflicting concerns. The assessment may also depend on the context: for example, content may be perceived as invitations to commit illegal activities in one context and serve a journalistic purpose in another.

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has stressed that the complex legal assessment of illegal content should *not* be delegated to companies and in this context has stated that:

"Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic."⁸⁸

In this context, it is key to distinguish between **the independent assessment** of whether the content is illegal on the one hand, and removal of content (**enforcement**) on the other.



Content that is "identical" or is "equivalent to" illegal content.

The mere **enforcement** corresponds to companies removing content following an order (or as appropriate under a general obligation). The enforcement case is best illustrated in the judgment by the European Court of Justice in **Glawischnig-Piesczek v. Facebook Ireland Limited**,⁸⁹ in which the Court found that a state can require Facebook to remove content which was previously declared to be illegal, or if the content "*is equivalent to*" content which was previously declared to be illegal. However, the Court stressed that the order must not require Facebook to carry out "*an independent assessment*" of the content.⁹⁰

A state's specific requests or general obligations for companies to remove illegal content is not in itself incompatible with human rights law. However, there may be requirements for how enforcement is to take place, for example how quickly companies should react when they become aware of illegal content.⁹¹

It is more unclear which conditions must be met when companies are to carry out an **independent assessment** of whether the content is illegal – as this assessment affects freedom of expression. As mentioned above, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression recommends that such decisions are not delegated to private companies.

When tech giants in practice are expected to **assess** large quantities of content in order to remove illegal content (either on the basis of a general obligation, a request or a recommendation, or on the basis of a voluntary agreement), there is a risk of over-regulation⁹², as companies would rather remove too much than too little content in order not to be held responsible and because they are rarely required to justify their decisions to users. **In practice** such over-regulation **can lead to restrictions on freedom of expression where legal content is removed.**⁹³

Delegating assessment to companies should therefore, as a minimum, require that a state supervise that the assessment is in accordance with human rights law.

Both over-regulation of content and massive data collection (see section 5.2) can lead to a *chilling effect* on freedom of expression and information. In its practice regarding freedom of expression, the European Court of Human Rights stresses that a state's interference with freedom of expression will not have a *chilling effect* on lawful expressions.⁹⁴

Overall, there is a risk that the state will set aside its responsibility for compliance with freedom of expression (and other human rights) by delegating its responsibility to private companies.⁹⁵

Concerns over having private actors assess whether content is illegal are increasingly relevant when the assessment is conducted via automated content filters and without subsequent human control, see section 5.2.1 on content filters.

Questions 2 and 3 are about the responsibility of companies and the state, respectively, when companies significantly impact society (**tech giants**). As

opposed to question 1, focus here is on the practice of companies regarding **legal content**.

Considering the important role that tech giants play for freedom of expression, several experts have recommended that **human rights protection be adapted to the digital era by committing tech giants to comply with human rights**. For example, today companies are not required to protect freedom of expression but can – based on their own terms and conditions – freely remove legal content.

One problem with leaving removal of **legal content** on the internet unregulated is that, in practice, companies play a central role for users' possibilities to enjoy their freedom of expression and information. Tech giants control the platforms, on which public debate takes place, and at the same time – based on their own terms and conditions – they are free to remove people as users of the platform and specific content.

In this connection, the Council of Europe has stated:

"(...) private entities can impose (and be 'encouraged' to impose) restrictions on access to information without being subject to the constitutional or international law constraints that apply to state limitations of the right to freedom of expression."⁹⁶

The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has stated that regulation of content should be based on human rights standards (A/74/486, point 42):

"When company rules differ from international standards, the companies should give a reasoned explanation of the policy difference in advance, in a way that articulates the variation. For example, were a company to decide to prohibit the use of a derogatory term to refer to a national, racial or religious group – which, on its own, would not be subject to restriction under human rights law – it should clarify its decision in accordance with human rights law."

Parts of the literature argue that – due to their significant role in society – tech giants should have a **legal obligation** to ensure freedom of expression on their platforms.⁹⁷

Others – such as the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression – have stated that the platforms should recognise that human rights are the global guidelines according to which they should organise their business. Specifically, the Special Rapporteur has recommended that the **UN Guiding Principles on Business and Human Rights** be used as a starting point, according to which companies should ensure that all parts of their business respect human rights. In this connection, companies should conduct regular human rights impact assessments and prevent the human rights risks that may be identified in such assessments. Furthermore, the Rapporteur recommended that companies operate on the basis of the principle of transparency and accountability.⁹⁸

As regards a **state's possible positive obligations** in relation to content regulation by tech giants of legal content (question 3), it has been stated that states should generally organise regulation of tech giants such that the protection of **freedom of expression is ensured in the best possible way**, for example by imposing requirements for increased **transparency** in content regulation by companies.⁹⁹

5.1.2 CHALLENGES IN ACCESS TO EFFECTIVE REMEDIES

In addition to grey areas in the substantial protection of freedom of expression, it is also difficult for users to gain access to **procedural protection**. Such protection follows from Article 13 of the European Convention on Human Rights and Article 47 of the Charter of Fundamental Rights of the European Union on the right to **an effective remedy** for everyone whose rights are violated.

A state's obligation to ensure an effective remedy is also an essential element in the UN Guiding Principles on Business and Human Rights, which stresses that companies also have a (non-judicial) responsibility to provide effective grievance mechanisms linked to their products and services.

The individual user will often not be aware that content has been removed because it was considered illegal, or because the content conflicted with the terms and conditions of the platform (or it was in a grey area between the two).

In situations where companies assess and remove content, the individual user does not have the same procedural right to challenge whether the content is protected under freedom of expression, as if the state itself had removed the content.¹⁰⁰ If the content was removed via content filters without human control, it may be unclear for the companies themselves why the content was removed (see more about content filters in section 5.1.2. below).

Added to this are situations in which companies delegate parts of the process to so-called "*trusted notifiers*".¹⁰¹ The EU defines "trusted notifiers" as individuals or organisations which are considered by the company to have particular expertise in assessing potentially illegal content.¹⁰²

The Danish Institute for Human Rights has previously [recommended](#) that an effective complaints system be ensured, which, as a minimum, entails that users are notified when their content is removed or blocked, they are informed about the basis for the decision, and given the opportunity to make objections within a reasonable period.



FACEBOOK OVERSIGHT BOARD

Facebook has established an independent oversight board of 40 members. The board is to serve as an "appeal body" in cases regarding removal of content and help ensure transparency in such cases. The board was established as part of Facebook's self-regulation and will settle principle cases on the basis of the terms and conditions of the platform, including balancing freedom of expression with other considerations and rights.¹⁰³

The board will only relate to content that *has* been removed and will not assess whether content still available on the platform should be removed.

It has been argued that Facebook's oversight board could become one of the most powerful enforcement bodies for freedom of expression – with jurisdiction across many countries. The board has been criticised for resembling a private tribunal that is not linked to the state and therefore is not obligated by fundamental procedural rules similar to those of other quasi-judicial authorities.¹⁰⁴



5.1.3 RISKS OF USING AUTOMATED CONTENT FILTERS

To a greater or lesser extent, tech giants use automated content filters for their content regulation. This applies to both illegal and legal content.¹⁰⁵

5.1.3.1 Automated content filters

Automated content filters are algorithms which **automatically identify and remove** – or prevent upload of – **content on the internet**. Content filters are based on **machine learning**, in which a self-learning algorithm analyses large amounts of data on content to find correlations and patterns in the data. These correlations and patterns can be used by the content filter to classify new examples that should be either removed or permitted.

In some cases, the results of the filter will subsequently be **reviewed by a human being** who will decide whether the content should actually be removed. In other cases, there is **no human control** of the content filter.

Algorithms **cannot understand specific circumstances** or contexts, even when these would be obvious to a human being. Therefore, even algorithmically sophisticated content filters developed on large high-quality datasets will always have **limited sorting accuracy**. This means that they will remove both too little and too much.¹⁰⁶

Moreover, a problem is that it is often **impossible to see why and how the filter has made a "decision"** to remove content.

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has stated that content filters pose specific human rights risks and that platforms should be aware of the limitations of automated solutions.¹⁰⁷

5.1.3.2 Upload filters

A noteworthy issue arises when automated **upload filters** or similar tools are used to block content or even prevent content from being uploaded to the platform.

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has stressed the challenges associated with this kind of "censorship", and has stated that, even if they are monitored by humans, such filters are unlikely to be compatible with freedom of expression because the interference involved is so severe that subsequent human control will not be able to compensate for it.¹⁰⁸

In light of this, the Danish Institute for Human Rights has previously [recommended](#) that *upload* filters not be used for content not previously assessed to be illegal when companies have taken "reasonable measures" to prevent illegal content or have otherwise complied with requirements to prevent illegal content. The institute has also recommended that assessment of whether content is illegal be made subject to regulatory supervision.

If, on the other hand, content has already been assessed to be illegal, upload filters may be used to prevent (re)upload of such content to the platform, and depending on the circumstances, the platform may be obligated to prevent such (re)upload.

CHRISTCHURCH

In 2019, there was a terrorist attack against the Al Noor Mosque in Christchurch, New Zealand. The attacker livestreamed the attack on his Facebook profile, and the video soon went viral on Facebook, YouTube, Twitter, Reddit and other platforms. Removing the video turned out to be a difficult task for the social media, because it was shared, downloaded and made available in different versions and sizes extremely quickly. The tech giants involved have since been criticised for not being effective enough in tracking down and removing the video, but also for allowing the video to find its way to the platforms in the first place.¹⁰⁹ In this connection, automated techniques and search methods can be necessary.¹¹⁰

5.1.3.3 Automated selection of content


The tech giants also use algorithms to select which content is to be made available to individual users. The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has stressed that use of artificial intelligence controls access to information in ways that are not transparent to the individual user, and sometimes not even to the platform itself. This may result in users being exposed to a limited range of important social or political stories, or not being exposed to such stories at all.¹¹¹

This issue is frequently referred to as **filter bubbles** or **echo chambers**, describing a situation where beliefs are reinforced by repetition. Ultimately, this can affect the **freedom of information**.¹¹²



FILTER BUBBLES AND ECHO CHAMBERS

Filter bubbles and echo chambers refer to a situation in which an algorithm seeks out information and presents it to the user based on information about the user available to the service (e.g. location, past search history, previous posts, etc.). Consequently, without noticing, the user is nudged towards news and debates that confirm the user's own opinions.¹¹³



The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has stressed the following:

"The intersection of technology and content curation raises novel questions about the types of coercion or inducement that may be considered an interference with the right to form an opinion."¹¹⁴

The Committee of Ministers of the Council of Europe has also warned against the potential manipulation of algorithmic processes, including their impact on human rights.¹¹⁵

It is unlikely that the tech giants will be required to completely abstain from using content filters, automated selection of content, etc., but minimum requirements for the use of such filters etc. could, and should, be imposed.

In this connection, it is worth considering whether regulation of tech giants' use of content filters, automated selection of content, etc. is possible through substantive and continuous human control of the automated systems and their development. Such human control should entail an efficient complaint system (see above) and comprehensive transparency reports with formal requirements for information to be disclosed by the platforms.¹¹⁶

5.2 THE RIGHT TO RESPECT FOR PRIVATE LIFE AND THE PROTECTION OF PERSONAL DATA

5.2.1 SURVEILLANCE CAPITALISM

The tech giants' business model is largely based on collection and use of as much information as possible about users. This information includes:

1. data intentionally disclosed by users, and
2. data unintentionally disclosed by users because the data can be derived from behaviour, search patterns, preferences, social networks, etc.¹¹⁷

This business model is especially applicable for tech giants such as Facebook and Google, because user data constitutes the (only) payment by users for using the companies' services and platforms. However, the business model represents a **market logic** that goes far beyond the tech giants.¹¹⁸

The market for trade in data also includes commercial actors such as *data brokers* collecting and selling data from various sources,¹¹⁹ and *ad-tech* firms offering specially designed analyses and tools for digital marketing.¹²⁰

The companies use the data collected to develop profiles of users, to predict their behaviour, to target marketing activities and to influence users in their purchases and opinions.¹²¹

Extensive collection and use of personal data have been referred to as **surveillance capitalism**.

Surveillance capitalism is characterised by companies collecting and generating data on all aspects of people's lives, including their experiences, preferences, social life, communication, consumption patterns, cultural and political activities, etc., and translating this data into products that can be sold. As part of this practice, surveillance capitalism **has created new products and markets**, based on the ability to predict and influence people's behaviour.

This situation is referred to as *ubiquitous surveillance*¹²³, because people are being surveilled in the digital as well as the physical world – and in the public as

well as the private sphere – via smartphones and the *internet of things devices*.¹²⁴

INTERNET OF THINGS (IOT)

The IoT is a technology that connects objects to the internet, enabling them to continuously submit relevant information. New "intelligent things" are constantly entering the market, widening the scope for surveilling and communicating with people's homes and cars, or monitoring their physical activity and sleep patterns. Since the technology is based on extensive collection and processing of personal data, the technological development raises new data protection challenges.

Comprehensive data collection by companies affects people's right to respect for private life and personal data.


The right to respect for private life and the protection of personal data provide broad protection for people's activity online. Such protection not only applies to the actual content of an email, for example, but also to metadata that can be analysed, aggregated and combined with other data, and thereby reveal information about the behaviour, social situation, personal preferences and identity of an individual.¹²⁵

Construction of detailed profiles can be used for *micro-targeting*.¹²⁶ One of the most well-known examples of micro-targeting is the Cambridge Analytica case, in which data collected via a Facebook app was used for voter targeting in the presidential election in the US. In October 2019, Facebook was fined GBP 500,000 for breach of the British Data Protection Act in connection with the Cambridge Analytica case.¹²⁷



CAMBRIDGE ANALYTICA

Cambridge Analytica was a British consultancy firm that provided analyses and consultancy to companies and political stakeholders in connection with targeted advertising. In 2018, it was revealed that Cambridge Analytica had collected personal data from 87 million Facebook users in connection with the US presidential election in 2016. The data was used to move undecided voters in American swing states to vote for Donald Trump.¹²⁸



It has been argued that the tech giants' business model is fundamentally at odds with the human rights protection of privacy.¹²⁹

The UN Special Rapporteur on the Right to Privacy has stated that:

"The tendency of Big Data to intrude into the lives of people by making their informational selves known in granular detail to those who collect and analyse their data trails is fundamentally at odds with the right to privacy and the principles endorsed to protect that right. Much of the economy of the modern Internet depends on harvesting complex data about potential customers in order to sell them things, a practice known as "Surveillance Capitalism". However, surveillance does not seem any more justifiable to data-driven efficiency than child-labour is to an industrial economy. It is only the most convenient and easiest way to exploit the information. It is not a fundamental right as is the right to privacy. Indeed, the data-driven economy would survive and prosper if minimal standards and improved technologies forced corporations and governments into a world in which ordinary people had much greater control over their own data."¹³⁰ (Notes have been omitted)

5.2.1.1 Lack of transparency

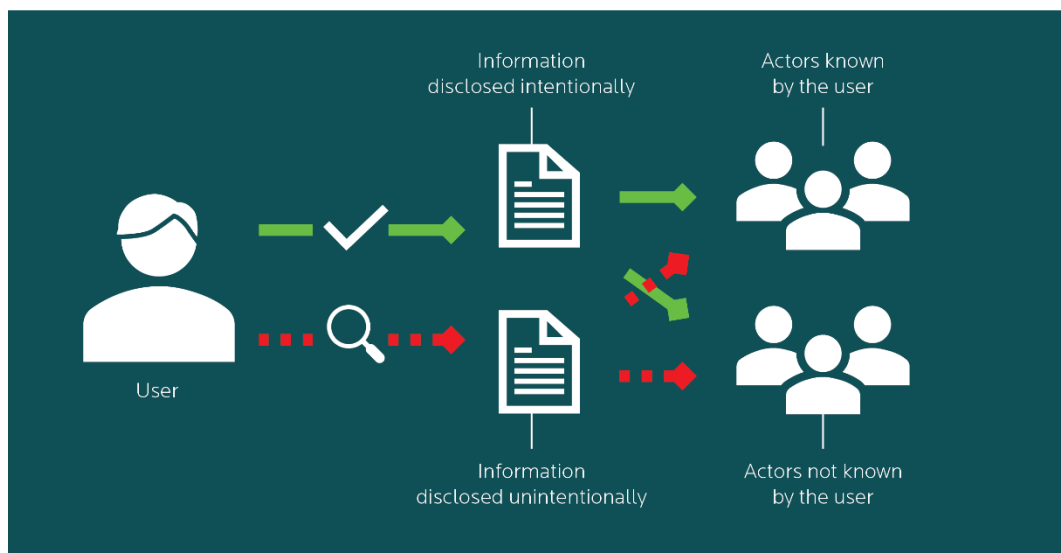
Extensive collection and use of information about users by tech giants reflect a non-transparent system challenging the right to privacy. The UN Special

Rapporteur on the Right to Privacy has stressed that a massive amount of data is being shared between companies (and countries), and individual users have no insight into this.¹³¹

The non-transparent interplay between the many actors on the market leads to a **loss of rights** which has been described as follows:

"When using available software and services online, users are defaulted into bundles of relationships with first- and third-party service providers, which are collecting their information in ways that leave little room for real choice or escape."¹³²

Thus, the current market structure means that data on individuals is being shared and used by many actors that the individual does not know about. The non-transparent relationships between actors mean that people do not know to whom they should direct any complaints.



5.2.1.2 Competition law as human rights protection

As this is a relatively new market, **the power of tech giants has also been examined in light of competition and consumer law**¹³³ and regulated through

protocols.¹³⁴ Initiatives in these areas may have a positive effect on human rights challenges.

For example, in a case concerning Facebook's strength on the market in terms of competition law, the German competition authorities pointed out that when access to personal data is crucial for a company's market strength (as is the case for Facebook), the issue of collecting and processing personal data is not merely a concern in terms of data protection law, but also a concern for competition law.¹³⁵ Lack of **transparency** with regard to companies' use of personal data can lead to unjustified competitive advantages.¹³⁶ As a result, it has been proposed that legislators work towards integrating competition law with the right to privacy and personal data, for example by competition authorities assessing **privacy and personal data as a competitive parameter**.¹³⁷

5.2.1.3 Increased risks due to automisation

The challenges for human rights law are exacerbated by the increased use and reuse of data resulting from tools based on artificial intelligence. The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression stressed this in a recent report on artificial intelligence:

"AI challenges traditional notions of consent, purpose and use limitation, transparency and accountability — the pillars upon which international data protection standards rest. Because AI systems work by exploiting existing datasets and creating new ones, the ability of individuals to know, understand and exercise control over how their data are used is deprived of practical meaning in the context of AI. Once data are repurposed in an AI system, they lose their original context, increasing the risk that data about individuals will become inaccurate or out of date and depriving individuals of the ability to rectify or delete the data."¹³⁸

Article 22 of the General Data Protection Regulation includes a **ban** against automated decisions that *significantly affect* the user. The ban applies to both public and private actors, but it remains unclear how "decisions" that "significantly affect" users is to be understood in terms of tech giants' collection and automated processing of personal data.

The Article 29 Working Party (now replaced by the European Data Protection Board) has stated that tech giants' marketing activities, which are often based on automated processing, are *not* considered to significantly affect the individual, and that consequently, **they are not prohibited under Article 22**. In some cases, however, the marketing activities **may affect users significantly**. This depends on 1) the "depth" of the profiling, including whether it involves tracking across different websites, units and services; 2) people's own expectations and wishes for the service; 3) the form of advertising; and 4) whether knowledge about users' potential vulnerabilities is exploited in the marketing.¹³⁹

There is no Danish or EU practice on the scope of the provision and how it is to be interpreted in relation to tech giants' collection and processing of personal data.

5.2.2 DATA PROTECTION CHALLENGES RELATED TO TECH GIANT PRACTICE

Tech giants' business model challenges several of the key principles of data protection law discussed below.

Tech giants' use of personal data can generally be divided into two purposes:


1. **Commercial purposes**, ranging from developing own services and products to selling products on to other private actors.
2. **Contributions to statutory tasks**, in particular police investigations, and to combatting crime or to intelligence activities.

The latter is outside the scope of this report, but note that with regard to state surveillance, including companies' disclosure of information to the authorities, the state is bound by its **human rights obligations**.¹⁴⁰



GLOBAL NETWORK INITIATIVE (GNI)

When tech giants receive requests from governments to provide information about an individual user, a certain degree of self-regulation takes place through the Global Network Initiative (GNI). Through membership of GNI, companies have committed themselves and each other to comply with human rights standards when receiving requests from governments involving privacy rights. The initiative has the limitation that it only concerns cases in which governments approach companies, and *not* cases in which the companies act on their own initiative. Consequently, the companies' own practice, for example in relation to collecting information on users for commercial purposes, is not covered by the initiative.



With regard to using personal data for **commercial purposes**, such use, including collection and disclosure of data, is subject to the regulations on the right to respect for private life and the protection of data by which private actors are bound.

The most relevant regulatory framework is the **General Data Protection Regulation (GDPR)**. The tech giants' access to information challenges, in particular, the GDPR requirements for **data minimisation, purpose limitation, (informed) consent and access**.¹⁴¹

5.2.2.1 Data minimisation

The requirement for **data minimisation**¹⁴² means that both the type and volume of personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are collected. This requirement means that companies are **not allowed to collect more personal data than is absolutely necessary**, and they are not allowed to collect information without any purpose (see section 5.2.2.2).

The data minimisation requirement is challenged by the common business model, which is based on collecting and generating as much knowledge as possible about the individual.¹⁴³

Furthermore, the level of accuracy and effectiveness of tools based on algorithms typically depends on large volumes of data, which again challenges the requirement of collecting and processing as little information as possible.¹⁴⁴

5.2.2.2 Purpose limitation

Further to this, the **purpose limitation** requirement¹⁴⁵ restricts companies' access to collect and process data. The requirement entails that personal data may only be collected for specified, explicit and legitimate purposes, and that data may not be further processed in a manner that is *incompatible* with the original purpose. Among other things, the purpose limitation requirement is to ensure that users can reasonably predict the scope and consequences of data processing.

In a business model in which tech giants collect and extract personal data from a large number of data points, the purpose limitation requirement will typically be addressed through descriptions of very broad data collection purposes in the terms of business. Such broad and imprecise purposes of data collection entail a risk of undermining the principle of purpose limitation.

5.2.2.3 Right of access

Pursuant to the data protection regulations, individuals have a right of access to their own data, and the right to know which personal data is being processed and who the data is being shared with. Among other things, this **right of access**¹⁴⁶ is to ensure that data processing is transparent for the individual user, and that the user is able to assess whether the data processing is reasonable and legitimate.

In practice, however, **information asymmetries** between individual users and tech giants are increasing. Users have very limited access to see which personal data the platforms are processing, especially the data and the profile generated on the basis of the individual's various online activities. You might say that the

tech giants know more and more about individual users, while individual users have limited access to the processing of data concerning themselves.

5.2.2.4 Consent

The possibility of individuals to control their own data is a key element in personal data protection, and in this context, **consent**¹⁴⁷ plays a crucial role as one of several means of authorising the processing of data. Consent is the individual's possibility to authorise data processing, and it should be a freely given, specific and informed indication of the individual's agreement to the processing of personal data.

The requirement for freely given, specific and informed consent is challenged by digital services because individual users often consent to the terms of the service without having insight into the conditions that they are consenting to. Because the platforms and services of the tech giants are so widespread and play such a crucial role for many people, individual users do not experience their consent as an actual (voluntary and informed) choice, but rather as a condition for joining relevant networks and debates, searching for information, etc.¹⁴⁸

Furthermore, individual users are not necessarily aware of the sometimes far-reaching consequences of giving consent, including onward sale and use of personal data for targeted marketing or profiling, because the consent is not described in plain and easy-to-read language on the platform. There is a risk of undermining the legal safeguards provided by the consent due to the length and complexity of the consent form and the number of times the user is asked to give consent (consent fatigue).¹⁴⁹ Moreover, it is unclear how the user's right to withdraw his or her consent can effectively be enforced in situations in which data about the user (including user profiles prepared by algorithmic tools) is disclosed to other commercial actors.¹⁵⁰

The consent requirements have been addressed by the French data protection agency **CNIL**, among others, and in 2019, the agency imposed a EUR 50 million fine on Google. This was the first fine issued by CNIL since the adoption of the General Data Protection Regulation, and according to CNIL, the size of the fine is based on the seriousness of the observed breaches of fundamental GDPR principles on transparency, information and consent.¹⁵¹

The consent requirements also played a key role when, in February 2020, the Danish Data Protection Agency raised serious criticisms of the Danish Meteorological Institute's use of personal data via banner ads from Google.¹⁵² In its decision, the Danish Data Protection Agency established that the Danish Meteorological Institute and Google have a financial interest in the data processing, and that the consent model on dmi.dk did not meet the statutory requirements for transparency, partly because it requires the user to take additional action in order to refuse giving consent. The option to refuse consent must therefore be stated as plainly and clearly as the option to give consent.

5.2.2.5 Lack of review by the European Courts

The question of tech giants' use of personal data for commercial purposes has neither been reviewed by the European Court of Human Rights (in terms of potential criminal liability) nor by the European Court of Justice (in terms of companies' obligations under EU law), but in individual member states, tech giants' obligations under EU law concerning the protection of privacy and personal data are being tried at national level.

As the European Courts have not yet examined the tech giants' behaviour with respect to the right to privacy and protection of personal data, protection varies between individual member states, and there is no common European understanding of the scope of personal data protection law.

A related problem is that it can be difficult for individual users to figure out how and where they should bring cases against tech giants. This problem is reflected in judgments by the European Court of Justice, for example **Google Spain, CNIL v. Google and Wirtschaftsakademie**. In an EU law context, the idea is for the European Data Protection Board to help align the rules.¹⁵³

CHAPTER 6

SELECTED PUBLICATIONS FROM THE DANISH INSTITUTE FOR HUMAN RIGHTS

6.1 FACT SHEETS

Fact sheet on automated content filters on online platforms (2019) (in Danish):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/policy_briefs/faktaark_om_automatiske_indholdsfilter_paa_digitale_platforme.pdf

Fact sheet on Council of Europe standards on technology and human rights (2019):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/faktaark_om_europaraadet_menneskerettigheder_og_teknologi.pdf

Fact sheet on UN standards on technology and human rights (2019) (in Danish):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/faktaark_ga/faktaark_om_fn_menneskerettigheder_og_teknologi_-_dansk_version.pdf

Fact sheet on privacy and data protection (2018) (in Danish):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/faktaark_ga/faktaark_om_databeskyttelse_og_rettet_til_privatliv.pdf

6.2 REPORTS

The Danish Institute for Human Rights (2019). Report on democratic participation on Facebook (in Danish):
https://menneskeret.dk/sites/menneskeret.dk/files/04_april_19/Rapport%20om%20demokratisk%20deltagelse.pdf

The Danish Institute for Human Rights (2017). Report on hate speech in the public online debate:

https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/ligebehandling_2017/rapport_om_hadefulde_ytringer_2._oplag_2017.pdf

6.3 CONSULTATION RESPONSES

The Danish Institute for Human Rights, consultation response concerning implementation of the carrying out AVMS Directive (2019) (in Danish):

<https://menneskeret.dk/hoeringssvar/gennemfoerelse-avms-direktivet>

The Danish Institute for Human Rights, consultation response concerning the regulation on preventing the dissemination of terrorist online content (2018) (in Danish):

<https://menneskeret.dk/hoeringssvar/hoering-forslag-forordning-forebyggelse-udbredelsen-terrorrelateret-online-indhold>

6.4 PUBLICATIONS

Jørgensen, Rikke Frank ed. (2019) *Human Rights in The Age of Platforms*, MIT Press:

<https://menneskeret.dk/udgivelser/human-rights-in-the-age-of-platforms>

Jørgensen, Rikke Frank (2017). Framing human rights: exploring storytelling within internet companies, *Information, Communication & Society*, 21:3, pp. 340-355:

<https://www.tandfonline.com/doi/full/10.1080/1369118X.2017.1289233>

Jørgensen, Rikke Frank (2017). What Platforms Mean When They Talk About Human Rights, *Policy and Internet*, 9:3, pp. 280-296:

<https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.152>

Jørgensen, Rikke Frank et al (2017). EU study on ICT and human rights (FRAME):

<https://www.humanrights.dk/publications/frame-ict-human-rights>

Jørgensen, Rikke Frank and Olsen, Birgitte Kofod eds. (2018). *Eksporeret - Grænser for privatliv i en digital tid*, Gads Forlag (in Danish):

<https://menneskeret.dk/udgivelser/eksporeret-graenser-privatliv-digital-tid>

Jørgensen, Rikke Frank and Pedersen, Anja Møller (2017). Online service providers as human rights arbiters in Taddeo & Floridi, *The Responsibilities of Online Service Providers*, Springer, pp. 179-199:

https://link.springer.com/chapter/10.1007/978-3-319-47852-4_10

Jørgensen, Rikke Frank and Zuleta, Lumi (2020). Private Governance of Freedom of Expression on Social Media Platforms. *Nordicom* 41(1):

<https://content.sciendo.com/view/journals/nor/41/1/article-p51.xml>

O'Brien, Claire Methven (2018), *Business and Human Rights – A Handbook for legal practitioners*, published by the Council of Europe:

<https://rm.coe.int/business-and-human-rights-a-handbook-of-legal-practitioners/168092323f>

¹ See Rikke Frank Jørgensen and Birgitte Kofod Olsen eds., *Eksporeret – grænser for privatliv i en digital tid*, Gads Forlag 2019 (in Danish).

² See the UN report on the rights to freedom of peaceful assembly and of association in the digital age A/41/41, 17 May 2019, available at: <https://undocs.org/A/HRC/41/41>

³ See for example the UN report on the right to freedom of opinion and expression A/73/348, point 17f., 28 August 2018, available at:

<https://undocs.org/A/73/348>

⁴ See for example the EU Action Plan against Disinformation (JOIN (2018) 36 final), available at:

https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf See also:

<https://menneskeret.dk/udgivelser/demokratisk-deltagelse-paa-facebook> (in Danish)

⁵ See for example: Communication from the Commission on Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe, COM(2016) 288 final, available at:

<https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.PDF>

⁶ See Joris van Hoboken: "The Privacy Disconnect" in Rikke Frank Jørgensen ed., *Human Rights in the Age of Platforms*, MIT Press 2019, pp. 255-284.

⁷ Jack M Balkin, "Old-School/New-School Speech Regulation" (2014), *Harvard Law Review* 127 (8):2296-234, available at:

<https://harvardlawreview.org/2014/06/old-schoolnew-school-speech-regulation/> See also: Rikke Frank Jørgensen ed., *Human Rights in the Age of Platforms*, MIT Press, 2019, pp. xvii-xlv.

⁸ Paul Nemitz, "Constitutional democracy and technology in the age of artificial intelligence" (2018) Vol. 376, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, available at:

<http://doi.org/10.1098/rsta.2018.0089>

⁹ See Emily Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, Cambridge University Press, 2015, pp. 44-57.

¹⁰ Rikke Frank Jørgensen, *Framing the Net: The Internet and Human Rights*, Edward Elgar 2013, pp. 93-95.

¹¹ See Martin Moore, *Tech Giants and Civic Power*, Kings College London, April 2016, available at:

<https://www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf>

¹² Amnesty International, *Surveillance Giants*, 2019, available at: <https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF> p. 11f.

¹³ See for example the UN reports A/HRC/29/31 and A/HRC/27/37, available at: <https://www.undocs.org/A/HRC/29/31> and at: <https://undocs.org/A/HRC/27/37>

¹⁴ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/74/486, available at: <https://undocs.org/en/A/74/486>. See also: Human Rights Committee's General Comment No. 34 (2011) on the two types of rights, available at: <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

¹⁵ See the Committee on the Elimination of Racial Discrimination General Recommendation No. 35 (2013), point 12, available at: <https://www.refworld.org/type,GENERAL,CERD,,53f457db4,0.html>

¹⁶ See the report of the UN Special Representative of the Secretary General, A/HRC/17/31, available at: https://www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf. See also: Stéphanie Lagoutte: *The State Duty to Protect Against Business-related human rights abuses*, DIHR Research Papers 2014/1, available at: <https://www.humanrights.dk/publications/state-duty-protect-against-business-related-human-rights-abuses>

¹⁷ See Nora Götzman ed., *Handbook on Human Rights Impact Assessment*, Edward Elgar, 2019.

¹⁸ See Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar" (*Facebook*, 2018), available at: <https://about.fb.com/news/2018/11/myanmar-hria/>

¹⁹ See Anne Mette Lauritzen and Frederik Stjernfelt, *Dit opslag er blevet fjernet*, Gyldendal, 2019, p. 171 (in Danish).

²⁰ See the report of the UN fact-finding mission on Myanmar, bottom of p. 14: A/HRC/39/64, available at: <https://undocs.org/en/A/HRC/39/64>

²¹ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/38/35, available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

²² See the report of the UN High Commissioner for Human Rights, A/HRC/39/29, available at: <https://undocs.org/A/HRC/39/29>. See also: Jørgensen, Rikke Frank and Lumi Zuleta (2020). Private Governance of Freedom of Expression on Social Media Platforms. *Nordicom* 41(1): <https://content.sciendo.com/view/journals/nor/41/1/article-p51.xml>

²³ See the ECHR case: *Times Newspapers Ltd v. United Kingdom*, paragraph 27, available at: [https://hudoc.echr.coe.int/eng#{"dmdocnumber":\["848220"\],"itemid":\["001-91706"\]}](https://hudoc.echr.coe.int/eng#{). For a complete overview of the practice of the European Court of Human Rights in relation to freedom of expression on the internet, see also Dirk Voorhoof, "Same standards, different tools? The ECtHR and the protection and limitations of freedom of expression in the digital environment" in *Human Rights Challenges in the Digital Age: Judicial Perspectives*, January 2020.

²⁴ See the ECHR case of *Delfi A/S v. Estonia*, paragraphs 115 and 116, available at: [https://hudoc.echr.coe.int/eng#{"itemid":\["001-155105"\]}](https://hudoc.echr.coe.int/eng#{). See also: The ECHR case of *Magyar Helsinki Bizottság v. Hungary*, available at: [https://hudoc.echr.coe.int/eng#{"itemid":\["001-167828"\]}](https://hudoc.echr.coe.int/eng#{) and the ECHR case of *Høiness v. Norway*, available at: [https://hudoc.echr.coe.int/eng#{"itemid":\["001-191740"\]}](https://hudoc.echr.coe.int/eng#{)

²⁵ See also the ECHR case of *Appleby et al v. United Kingdom*, paragraphs 47-49, available at: [https://hudoc.echr.coe.int/eng#{"itemid":\["001-61080"\]}](https://hudoc.echr.coe.int/eng#{). See also: The Council of Europe 2011 research report "Positive obligations on member states under Article 10 to protect journalists and prevent impunity", pp. 4-5, available at: https://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf

²⁶ See the ECHR case of *Von Hannover v. Germany*, available at: [https://hudoc.echr.coe.int/eng#{"itemid":\["001-61853"\]}](https://hudoc.echr.coe.int/eng#{), the ECHR case of *Couderc v. France*, available at: [https://hudoc.echr.coe.int/eng#{"itemid":\["001-158861"\]}](https://hudoc.echr.coe.int/eng#{), and the ECHR case of *Delfi v. Estonia*, available at: [https://hudoc.echr.coe.int/eng#{"itemid":\["001-155105"\]}](https://hudoc.echr.coe.int/eng#{).

²⁷ Jon Kjølbros, *Den Europæiske Menneskerettighedskonventionen – for praktikere* (4th edition). Djøf Forlag, 2017, p. 798 (in Danish).

²⁸ Jon Kjølbros, *Den Europæiske Menneskerettighedskonventionen – for praktikere* (4th edition).

Djøf Forlag, 2017, p. 800 (in Danish) with reference to the ECHR case of K.U. v. Finland, paragraphs 40-51, available at:

[https://hudoc.echr.coe.int/eng#{"itemid":\["001-89964"\]}](https://hudoc.echr.coe.int/eng#{)

²⁹ Jon Kjølbros, *Den Europæiske*

Menneskerettighedskonventionen – for praktikere (4th edition).

Djøf Forlag, 2017, p. 802 (in Danish).

³⁰ See the ECHR case of Paksas v. Lithuania, paragraph 88, available at:

[https://hudoc.echr.coe.int/eng#{"itemid":\["001-102617"\]}](https://hudoc.echr.coe.int/eng#{). See

also: Jon Kjølbros, *Den Europæiske*

Menneskerettighedskonvention – for praktikere (4th edition).

Djøf Forlag, 2017, p. 1073.

³¹ See in particular the ECHR case of S & Marper v. United Kingdom, available at:

[https://hudoc.echr.coe.int/eng#{"itemid":\["001-90051"\]}](https://hudoc.echr.coe.int/eng#{). For

an overview of the practice of the European Court of Human

Rights in relation to protection of personal data, see also the

Court's fact sheet of October 2019, available at:

https://www.echr.coe.int/Documents/FS_Data_ENG.pdf

³² See the ECHR case of Satakunnan v. Finland, paragraph 137, available at:

[https://hudoc.echr.coe.int/eng#{"itemid":\["001-175121"\]}](https://hudoc.echr.coe.int/eng#{)

³³ See the ECHR case of M.S. v. Sweden, paragraph 35, available at:

[https://hudoc.echr.coe.int/eng#{"itemid":\["001-58177"\]}](https://hudoc.echr.coe.int/eng#{), and

the ECHR case of Perry v. United Kingdom, paragraph 39ff,

available at:

[https://hudoc.echr.coe.int/fre#{"itemid":\["001-61228"\]}](https://hudoc.echr.coe.int/fre#{)

³⁴ See the ECHR case of Perry v. United Kingdom, paragraph 48, available at:

[https://hudoc.echr.coe.int/fre#{"itemid":\["001-61228"\]}](https://hudoc.echr.coe.int/fre#{)

³⁵ See the ECHR case of Centrum För Rättvisa v. Sweden, available at:

[https://hudoc.echr.coe.int/eng#{"itemid":\["001-183863"\]}](https://hudoc.echr.coe.int/eng#{), and

Big Brother Watch et al v. United Kingdom, available at:

[https://hudoc.echr.coe.int/eng#{"itemid":\["001-186048"\]}](https://hudoc.echr.coe.int/eng#{)

³⁶ See the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (1981), available at:

<https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>

³⁷ Recommendation of the Committee of Ministers of the Council of Europe, CM/Rec(2008)6, available at:

<https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/>

[/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2008-6-of-the-committee-of-ministers-to-member-states-on-measures-to-promote-the-respect-for-freedom-of-expression-and-informati?inheritRedirect=false](#)

³⁸ Recommendation of the Committee of Ministers of the Council of Europe, CM/Rec(2016)3, available at: <https://edoc.coe.int/en/fundamental-freedoms/7302-human-rights-and-business-recommendation-cmrec20163-of-the-committee-of-ministers-to-member-states.html>. See also: Claire Methven O'Brien, *Business and Human Rights, a handbook for legal practitioners*, (CoE, 2018), available at:

<https://rm.coe.int/business-and-human-rights-a-handbook-of-legal-practitioners/168092323f>

³⁹ See Council of Europe resolution 1843(2011) on the protection of privacy and personal data on the Internet and online media, available at:

<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=18039&lang=en>

⁴⁰ See Council of Europe resolution 2311 "Human rights and business – what follow-up to Committee of Ministers Recommendation CM/Rec(2016)3?" available at:

<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28296&lang=en>

⁴¹ A full overview of standards related to article 8 is available at: <https://www.coe.int/en/web/portal/personal-data-protection-and-privacy>, and an overview related to article 10 is available at:

<https://www.coe.int/en/web/portal/protecting-freedom-of-expression-and-information>

⁴² See the Charter of Fundamental Rights of the European Union (2010/C 83/02), available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12010P&from=EN>

⁴³ See the Directive on electronic commerce 2000/31/EC, available at:

<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031>

⁴⁴ See also: Thomas Riis et al "Leaving the European Safe Harbor, Sailing Towards Algorithmic Content Regulation", *Journal of Internet Law*, Vol. 22, No. 7, 2019, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300159

⁴⁵ See the background paper from the European Parliament of 20 May 2020, available at:

[https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA\(2020\)649404_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf)

⁴⁶ See Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, available at:

<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32011L0093>

⁴⁷ See Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790>

⁴⁸ See Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on audiovisual media services, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L1808&from=DA>

⁴⁹ See the judgment of the European Court of Justice in C-70/10 (SABAM v. Scarlet Extended), available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0070&from=DA>, see also: C-360/10, dealing with the same issue:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1499753>. The scope of Article 15 is also considered in C-484/14 and C-324/09.

⁵⁰ See the judgment of the European Court of Justice in C-70/10 (SABAM v. Scarlet Extended), paragraph 40, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0070&from=DA>

⁵¹ See judgment of European Court of Justice in C-70/10 (SABAM v. Scarlet Extended), paragraph 50, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0070&from=DA>

⁵² See the judgment of the European Court of Justice in C 18/18 (Glawischnig-Piesczek v. Facebook Ireland Limited), available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1501064>

⁵³ See the judgment of the European Court of Justice in C 18/18 (Glawischnig-Piesczek v. Facebook Ireland Limited), paragraph 45 available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1501064>

⁵⁴ See the judgment of the European Court of Justice in C 18/18 (Glawischnig-Piesczek v. Facebook Ireland Limited), paragraph 46 available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1501064>

⁵⁵ See the EU General Data Protection Regulation (GDPR) 2016/679, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

⁵⁶ See also: The Article 29 Working Party's statement no. 4/2007 on the concept of personal data, available at:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_da.pdf

⁵⁷ Act on supplementary provisions for the regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Danish Data Protection Act), available (in Danish) at:

<https://www.retsinformation.dk/Forms/r0710.aspx?id=201319>

⁵⁸ See Directive 2002/58/EF of the European Parliament and of the Council of 12 July 2002 concerning the protection of privacy in the electronic communications sector, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=DA>

⁵⁹ See the statement of the European Data Protection Board on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, available at:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf

⁶⁰ See the judgment of the European Court of Justice in the joined cases C-203/15 (Tele2 Sverige AB v. Post- och telestyrelsen) and C-698/1 (Secretary of State for the Home Department v. Tom Watson et al), available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN>

⁶¹ See the judgment of the European Court of Justice in C-673/17 (Planet49), available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7376436>

⁶² See the judgment of the European Court of Justice in C-131/12 (Google Spain), available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7376861>

⁶³ See the judgment of the European Court of Justice in C-131/12 (Google Spain), paragraph 80f., available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7376861>

⁶⁴ See the judgment of the European Court of Justice in C-131/12 (Google Spain), paragraph 88, available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7376861>

⁶⁵ See the judgment of the European Court of Justice in C-507/17 (CNIL v. Google), available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=7377476>

⁶⁶ See the judgment of the European Court of Justice in C-507/17 (CNIL v. Google), paragraph 60, available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=7377476>

⁶⁷ See the judgment of the European Court of Justice in C-507/17 (CNIL v. Google), paragraph 67, available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=7377476>. See also: Christopher Docksey, "The EU approach to the protection of rights in the digital environment: today and tomorrow – State obligations and responsibilities of private parties – GDPR rules on data protection, and what to expect from the upcoming ePrivacy regulation" in *Human Rights Challenges in the Digital Age: Judicial Perspectives* (CoE 2020).

⁶⁸ See the judgment of the European Court of Justice in C-210/16 (Wirtschaftsakademie), available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7019567>

⁶⁹ To read more about the issue of jurisdiction and enforcement of human rights in the digital environment, see *Human Rights Challenges in the Digital Age: Judicial Perspectives* (CoE & ECoHR 2020)

⁷⁰ See the judgment of the European Court of Justice in C-362/14 (Maximillian Schrems), available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7378769>

⁷¹ The Commission Decision of 26 July 2000 (on the safe harbour privacy principles) is available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520&from=en>

⁷² See the judgment of the European Court of Justice in C-362/14 (Maximillian Schrems), paragraph 78, available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7378769>

⁷³ See the opinion of the Advocate General concerning the judgment in C-311/18, available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=471129>

⁷⁴ See the judgment of the European Court of Justice in C-40/17 (Fashion ID), available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7380173>

⁷⁵ See the judgment of the European Court of Justice in C-40/17 (Fashion ID), paragraph 101, available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7380173>

⁷⁶ See the judgment of the European Court of Justice in C-40/17 (Fashion ID), paragraph 102 ff, available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7380173>

⁷⁷ See the cooperation agreement on combatting hate speech online, available at:

https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

⁷⁸ See the Commission's work on responsibilities and duties in relation to online platforms, available at:

<https://ec.europa.eu/digital-single-market/en/online-platforms-digital-single-market>

⁷⁹ Commission Recommendation 2018/334 of 1 March 2018 (on measures to effectively tackle illegal content online) is available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0334&from=en>

⁸⁰ The report from the Commission on Freedom of Expression is available (in Danish) at:

https://www.justitsministeriet.dk/sites/default/files/media/Pre_smeddelelser/pdf/2020/betaenkning_nr_1573_2020_del_1.pdf

⁸¹ See the reply from the Danish Minister for Justice to the Legal Affairs Committee to *REU (Alm. del)*, question no. 355 of 15 October 2019, available (in Danish) at:

<https://www.ft.dk/samling/20182/almdel/reu/spm/355/index.htm>

⁸² See also the reply from the Danish Minister for Justice of 24 October 2019 to question no. 363 (*Alm. del*), available (in Danish) at:

<https://www.ft.dk/samling/20182/almdel/reu/spm/363/svar/1600521/2094110.pdf>

⁸³ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/38/35, available at:

<https://undocs.org/en/A/HRC/38/35>

⁸⁴ See for example the ECHR case of the *Sunday Times v. United Kingdom*, paragraphs 47-49, available at:

[https://hudoc.echr.coe.int/rus#{"itemid":\["001-57584"\]}](https://hudoc.echr.coe.int/rus#{)

⁸⁵ See the EU study on ICT and human rights (FRAME) 2017, p. 27, available at:

<https://www.humanrights.dk/publications/frame-ict-human-rights>

as well as the annex to the Council of Europe Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, point 1.1.1.

⁸⁶ See in particular *The Rise of Content Cartels*, Evelyn Douek, available at:

<https://knightcolumbia.org/content/the-rise-of-content-cartels>

⁸⁷ See Rikke Frank Jørgensen, *Rights Talk: In the Kingdom of Online Giants*, in *Human Rights in the Age of Platforms*, MIT Press, 2019, pp. 163-187. See also: Rikke Frank Jørgensen, "What platforms mean when they talk about human rights", *Internet Policy*, Vol. 9, issue 3, 2017, pp. 280-296.

⁸⁸ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/38/35, p. 7, available at:

<https://undocs.org/en/A/HRC/38/35>

⁸⁹ See the judgment of the European Court of Justice in *C 18/18 (Glawischnig-Piesczek v. Facebook Ireland Limited)*, available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1501064>

⁹⁰ See the judgment of the European Court of Justice in C 18/18 (Glawischnig-Piesczek v. Facebook Ireland Limited), paragraph 45 available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1501064>

⁹¹ Jacob Mchangama, "Nu skal danske politikere holde tungen lige i munden – ellers kan det gå hårdt ud over din ytringsfrihed", Berlingske, 18 February 2020. The article is available (in Danish) at:

<https://www.berlingske.dk/kommentatorer/nu-skal-danske-politikere-holde-tungen-lige-i-munden-ellers-kan-det>

⁹² See for example Daphne Keller, "Empirical evidence of 'overremoval' by Internet Companies under Intermediary Liability Laws" (The Center for Internet and Society), available at:

<http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws>

⁹³ Report from the Committee of experts to the Council of Europe, MSI-NET (2016) 06 re 3 Final, Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, p. 20, available at:

<https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a>

⁹⁴ See for example the ECHR case of Pedersen and Baadsgaard v. Denmark, paragraph 93, available at:

https://menneskeret.dk/sites/menneskeret.dk/files/afgoerelsesdatabase/2004-12-17_49017.99_pedersen_and_baadsgaard_v_denmark.pdf

⁹⁵ See Daphne Keller, "Who do You Sue? State and Platform Hybrid Power Over Online Speech" (2019, Hoover Institution), available at:

<https://www.hoover.org/research/who-do-you-sue>

⁹⁶ See the Council of Europe Commissioner for Human Rights, "The rule of law on the Internet and in the wider digital world" (CoE, 2014), available at:

<https://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf> See also: Felix Schwemer, "Trusted notifiers and the privatization of online

enforcement", *Computer Law & Security Review*, Vol. 35, Issue 6 (2019), available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3287754

⁹⁷ Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation 2018*, p. 1194, and Molly K. Land in *Regulating Private Harms Online: Content Regulation under Human Rights Law in Human Rights in the Age of Platforms*, ed. Rikke Frank Jørgensen, 2019, and Emily Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, Cambridge University Press 2015. See also: Angelopoulos et al in "Study of fundamental rights framework for self-regulation and privatized enforcement online", 2017, and Laidlaw: "Online Platform Responsibility and Human Rights" in *Platform Regulations: How Platforms are Regulated and How They Regulate Us. Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility*, 2017.

⁹⁸ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/38/35, available at:

<https://undocs.org/en/A/HRC/38/35> See also: A/HRC/32/38, available at:

<https://undocs.org/en/A/HRC/32/38>, and A/73/348, available at:

<https://undocs.org/en/A/73/348>

⁹⁹ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/38/35, A/HRC/32/38 and A/73/348. See also: Wagner et al "Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act", *ACM Conference on Fairness, Accountability, and Transparency (2020)*, available at:

https://www.researchgate.net/publication/338802975_Regulating_Transparency_Facebook_Twitter_and_the_German_Network_Enforcement_Act

¹⁰⁰ Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation 2018*, p. 1177.

¹⁰¹ Schwemer, *Trusted notifiers and the privatization of online enforcement*, November 2019, in: *Computer Law & Security Review*.

¹⁰² See Commission Recommendation 2018/334 on measures to effectively tackle illegal content online, point 4(g), available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0334>

¹⁰³ See Facebook news item

<https://about.fb.com/news/2019/09/oversight-board-structure/>, and Mark Zuckerberg's letter

<https://about.fb.com/wp-content/uploads/2019/09/letter-from-mark-zuckerberg-on-oversight-board-charter.pdf>

¹⁰⁴ See "Some questions regarding Facebook's oversight board and remediation of human rights impacts", part I and part II, available at:

<http://opiniojuris.org/2020/03/03/some-questions-regarding-facebooks-oversight-board-and-remediation-of-human-rights-impacts-part-i/> and

<http://opiniojuris.org/2020/03/04/some-questions-regarding-facebooks-oversight-board-and-remediation-of-human-rights-impacts-part-ii/>

¹⁰⁵ Report from the Committee of experts to the Council of Europe, MSI-NET (2016) 06 re 3 Final, Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, p. 18, available at:

<https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a>

¹⁰⁶ See the Council of Europe, "Study on the Human Rights Dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications" (CoE, 2016), available at:

<https://rm.coe.int/draft-study-on-the-human-rights-dimensions-of-automated-data-processin/168075c4da>

¹⁰⁷ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348, available at:

<https://undocs.org/pdf?symbol=en/A/73/348>

¹⁰⁸ See the letter from the Special Rapporteur of 13 June 2018, available at:

<https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf> See also the note by the UN Special

Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348, items 16 and 40, available at:

<https://undocs.org/A/73/348>

¹⁰⁹ See Thomas Aagaard, "Terror i Christchurch: Derfor er det så svært at fjerne massakrevideoen fra nettet", *Berlingske*, 19 March 2019, available (in Danish) at:

<https://www.berlingske.dk/internationalt/terror-i-christchurch-derfor-er-det-saa-svaert-at-fjerne>

¹¹⁰ See the judgment of the European Court of Justice in C 18/18 (Glawischnig-Piesczek v. Facebook Ireland Limited), paragraph 46 available at:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1501064>

¹¹¹ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348, available at:

<https://undocs.org/pdf?symbol=en/A/73/348>

¹¹² See the Council of Europe, "Study on the Human Rights Dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications" (CoE, 2016), available at:

<https://rm.coe.int/draft-study-on-the-human-rights-dimensions-of-automated-data-processin/168075c4da>, see also: Anne Mette Lauritzen and Frederik Stjernfelt, *Dit opslag er blevet fjernet*, Gyldendal, 2019, p. 45ff (in Danish).

¹¹³ See Nationalt Center for Forebyggelse af Ekstremisme, *Ekkokamre*, 7. August 2019 (in Danish):

<https://stopekstremisme.dk/ekstremisme/opslagsvaerk/ekkokamre>

¹¹⁴ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348, paragraph 24, available at:

<https://undocs.org/pdf?symbol=en/A/73/348>

¹¹⁵ See the declaration by the Council of Europe on the manipulative capabilities of algorithmic processes, February 2019, available at:

https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b. See also: Amnesty International, *Surveillance Giants*, 2019, available at:

<https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF> p. 35f.

¹¹⁶ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348, available at:

<https://undocs.org/pdf?symbol=en/A/73/348>

¹¹⁷ See Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019.

¹¹⁸ See Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019.

¹¹⁹ See Annex 4 to UN report A/HRC/62, available at:

<https://undocs.org/A/HRC/37/62>

- ¹²⁰ "How do data companies get out data?" (*Privacy International* 2018), available at:
<https://privacyinternational.org/long-read/2048/how-do-data-companies-get-our-data>
- ¹²¹ See the Article 29 Working Party's opinion 2/2010 on online behavioural advertising, available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf
- ¹²² Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019.
- ¹²³ See Amnesty International, *Surveillance Giants*, 2019, available at:
<https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>
- ¹²⁴ See the Article 29 Working Party's opinion 8/2014 on recent developments on the Internet of Things, available at:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
- ¹²⁵ See the judgment of the European Court of Justice in the joined cases C-203/15 (Tele2 Sverige AB v. Post- och telestyrelsen), C-698/1 (Secretary of State for the Home Department v. Tom Watson et al), available at:
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN>, UN report A/HRC/39/29, available at:
<https://undocs.org/A/HRC/39/29> and A/HRC/27/37, paragraph 19, available at:
<https://undocs.org/A/HRC/27/37>
- ¹²⁶ See Amnesty International, *Surveillance Giants*, 2019, available at:
<https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF> pp. 29-33.
- ¹²⁷ See for example Thomas Breinstrup, "Facebook betaler millionbøde for datamisbrug" (*Berlingske*, 2019), available (in Danish) at:
<https://www.berlingske.dk/virksomheder/facebook-betaler-millionboede-for-datamisbrug>
- ¹²⁸ See Anne Mette Lauritzen and Frederik Stjernfelt, *Dit opslag er blevet fjernet*, Gyldendal, 2019, p. 16f (in Danish).
- ¹²⁹ See for example Amnesty International, *Surveillance Giants*, 2019, available at:
<https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF> p. 25f, and UN report A/HRC/27/37, paragraph 2, available at:
<https://undocs.org/A/HRC/27/37>

¹³⁰ See the report of the Special Rapporteur on the Right to Privacy A/HRC/37/62, annex 2, available at:

<https://undocs.org/A/HRC/37/62>

¹³¹ See UN report A/HRC/39/29, available at:

<https://undocs.org/A/HRC/39/29>

¹³² See Joris van Hoboken, "The Privacy Disconnect", in *Human Rights in the Age of Platforms*, ed. Rikke Frank Jørgensen, MIT Press 2019, pp. 255-285. See also: Bennett Cyphers et al "Behind the One-Way Mirror, a deep dive into the technology of corporate surveillance", *Electronic Frontier Foundation*, 2019. The report is available at:

<https://www.eff.org/document/behind-one-way-mirror-deep-dive-technology-corporate-surveillance>

¹³³ See the European Data Protection Supervisor's Opinion 8/2016, available at:

https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf, the European Data Protection

Board's statement, available at:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf and the European

Commission's report, "Shaping Europe's Digital Future" 2019, available at:

https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

¹³⁴ Mike Masnick, "Protocols, Not Platforms: A Technological Approach to Free Speech", 21 August 2019, available at:

<https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech>

¹³⁵ The decision by the German data protection agency is available at:

https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html. For a

description of the case, see for example:

<https://www.slaughterandmay.com/media/2536711/facebook-germany-a-new-frontier-for-privacy-and-competition.pdf>

¹³⁶ See the European Data Protection Supervisor's Opinion 8/2016, available at:

https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf and "Competition and data"

(*Privacy International*), available at:

<https://www.privacyinternational.org/explainer/2293/competition-and-data>

¹³⁷ "Tech companies are trying to redefine privacy – what's missing is real competition on privacy" (*Privacy International*, 2019), available at:

<https://privacyinternational.org/long-read/2939/tech-companies-are-trying-redefine-privacy-whats-missing-real-competition-privacy>

¹³⁸ See the report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348, paragraph 35, available at:

<https://undocs.org/pdf?symbol=en/A/73/348>

¹³⁹ See the Article 29 Working Party's Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, p. 23, available at:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

¹⁴⁰ For a review of authorities' access to surveillance of people's online behaviour, see the report by Henrik Udsen, *Danske myndigheders registrering af borgernes adfærd på internettet – regelgrundlaget og de tilhørende kontrolmekanismer*, June 2017, available (in Danish) at:

http://justitia-int.org/wp-content/uploads/2017/06/Rapport_Danske-myndigheders-registrering-af-borgernes-adfærd-på-internettet_14-06-17.pdf

¹⁴¹ For a review of data protection rules pursuant to the GDPR, see Birgitte Kofod Olsen, *Håndbog i Data Ansvarlighed*, Djøfs Forlag, 2019 (in Danish).

¹⁴² Article 5(1)(c) of the General Data Protection Regulation.

¹⁴³ See Rikke Frank Jørgensen and Tariq Desai, "Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google", *Nordic Journal of Human Rights*, Vol. 35, No. 2., 2017, pp. 106-126.

¹⁴⁴ See the report from the Norwegian data protection agency on data protection law challenges related to Big Data, September 2013, available (in Norwegian) at:

<https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/big-data/>

¹⁴⁵ Article 5(1)(b) of the General Data Protection Regulation.

¹⁴⁶ Article 15 of the General Data Protection Regulation.

¹⁴⁷ Article 6(1)(a), and Article 9(2)(a) of the General Data Protection Regulation. See also Article 7.

¹⁴⁸ See "Competition and data" (*Privacy International*), available at:

<https://www.privacyinternational.org/explainer/2293/competition-and-data>.

The General Data Protection Regulation requirement for consent is the focal point of an ongoing case raised by the noyb.eu organisation against Google, Instagram, WhatsApp and Facebook. The case is described here:

<https://noyb.eu/en/gdpr-noybeu-filed-four-complaints-over-forced-consent-against-google-instagram-whatsapp-and>

¹⁴⁹ See Lilian Edwards, Privacy, Law, Code and Social Networking Sites, in Research handbook on governance of the internet (Ian Brown ed., Edward Elgar, 2013), Rikke Frank Joergensen, The Unbearable Lightness of User Consent, in 3 Internet policy review 4 (2014); Brendan Van Alsenoy et al, Privacy notices versus informational self-determination: Minding the gap, in 28 International Review of Law, Computers & Technology 2, 185–203 (2014).

¹⁵⁰ The role of the courts in addressing the human rights implications of new and emerging technologies in Human Rights Challenges in the Digital Age: Judicial Perspectives (CoE & ECoHR 2020).

¹⁵¹ See "The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC" (CNIL, 2019), available at:

<https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>. For a review of 13 cases of privacy complaints against Google and Facebook in the period from 2011 to 2016, see Rikke Frank Jørgensen and Tariq Desai, "Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google", *Nordic Journal of Human Rights*, Vol. 35, No. 2, 2017, pp. 106-126, available at: <https://www.tandfonline.com/doi/full/10.1080/18918131.2017.1314110>

¹⁵² The decision by the Danish Data Protection Agency of 11 February 2020 concerning the Danish Meteorological Institute's processing of personal data about website visitors, available (in Danish) at:

<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/feb/dmis-behandling-af-personoplysninger-om-hjemmesidebesoegende/>

¹⁵³ See the reply (in Danish) from the Danish Minister for Justice to question 711 from the Legal Affairs Committee concerning a common European system:

<https://www.ft.dk/samling/20191/almdel/reu/spm/711/svar/1632156/2146952/index.htm>. See also: Strategy paper from the European Commission, "A European Strategy for Data", available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf