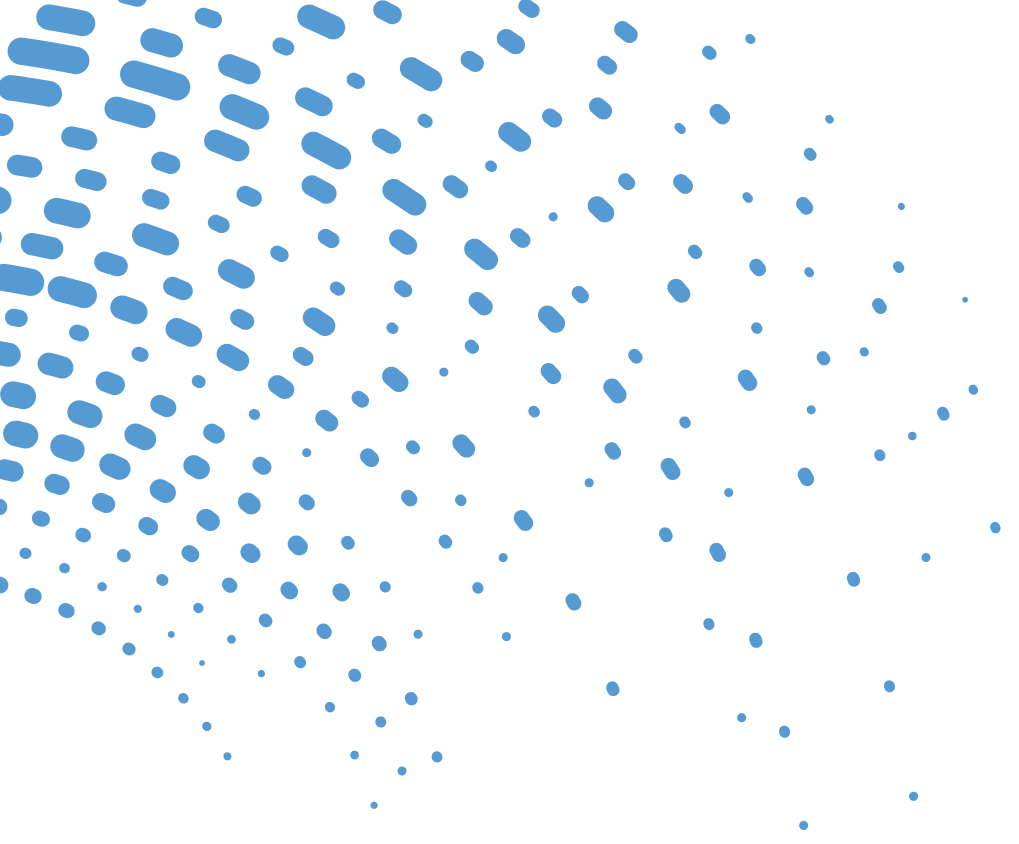


Ensuring democracy and freedom of speech online

– a need for a balanced regulation of social networks

“Our democracies are challenged.
The same social networks that have given the voiceless an opportunity to express themselves, and which give us all opportunities for contact and friendship, are also used by those who manipulate millions of people through false campaigns, and inciting hatred.
We as publishers must engage in the discussion of how to balance necessary measures to protect democracy and an equally necessary protection of freedom of speech.”

Kristin Skogen Lund, CEO of Schibsted

Background

Representatives of the EU Commission have encouraged Schibsted to share its views on the regulation of social networks as input for the upcoming discussions on regulating of digital services and tackling the negative consequences of social networks in the information ecosystem. Schibsted is a media group primarily operating in Norway, Sweden and Finland. The group owns some of the largest media houses in Norway and Sweden. It also operates online marketplaces for trading products and services, as well as growth companies for online services in all three countries. In addition, Schibsted holds 60 percent of Adevinta´s shares, an international online marketplace group, founded by Schibsted. Adevinta was listed on the Oslo Stock Exchange in April 2019.

Schibsted has developed its values through 170 years of free and independent newspapers, founded on a strong awareness of the social responsibility that comes with this task. The principal owner, Tinius Trust, is also safeguarding that these values are upheld in a complex digital world. Tinius Trust owns a controlling stake of 26 percent in Schibsted and was established by principal owner Tinius Nagell Erichsen in 1996.

In the Tinius Trust Articles of Association it says: “The Schibsted Group is run in such a way that it ensures free and independent editing of the newspapers owned by the Group and its subsidiaries involved in editorial operations. The Schibsted Group strives for quality and credibility in all its publications, and defends such values as religious freedom, tolerance, human rights and democratic principles. “ We at Schibsted want to contribute to the debate on regulating platforms within the EU by bringing a publisher’s perspective to the discussion. The necessity to protect democracy against the severe effects of disinformation and hate, whilst ensuring it is done in a way that does not restrict publishers, or individual’s freedom of expression, has been the guiding principle for this report.

Table of contents

1. Executive summary

The rise of social networks has revolutionized and transformed the information sphere. Social networks have given people new means of expressing themselves, and of accessing information. But they have also created problems, that our societies need to deal with.

The trends we see in today's connected world have severe consequences. Disinformation campaigns conveyed through social networks may interfere with elections, incite violence and even genocide, paralyze democratic institutions and silence politicians and public-sector employees.

Looking ahead, the improved quality of personal data accessible to social networks, the development of AI, more technically sophisticated possibilities for manipulation (deepfakes), will in all likelihood contribute to an escalation of the negative trends we identify in this report. It is urgent to address the problems at hand while it is still possible.

The discussion about regulating platform liability and tackling digital manipulation in Europe is ongoing in many Member States and has also occupied the EU institutions during the last years. As the EU Commission is thinking about its future approach on this matter, Schibsted wants to contribute to the debate by issuing this report. Our objective with the report is to describe our view on these matters and propose regulation of social networks that reduces the negative impact for democracy and democratic institutions, without compromising the freedom of expression of citizens, or leading to regulatory overreach for publishers with editorial responsibility.

Schibsted believes that in order to limit the consequences of these problems it is necessary to define social networks as a new category in mass communication, with a specific type of secondary liability. Social networks are not publishers and lack editorial responsibility. Therefore, they should not be regulated as publishers, but as a new category of players placed between publishers of journalistic content with full responsibility for the content they produce, and telecom companies, that are distributing content.

We believe that this central part of the connected society cannot be left to voluntary systems of company-level self-regulation but should be subject to legal accountability and regulatory scrutiny in order to protect democracy and freedom of speech online.

In this report Schibsted acknowledges that there are many rules already in place for social networks, both on EU and national level. National criminal codes regulate many aspects of harm affecting democratic institutions and free elections, but the networks' responsibilities under these sections are in many aspects still unclear and there is almost no court practice in this field.

Photo:
Carson Arias

In addition, there is a need to enhance rules for liability and transparency of these networks in order to have a functional online space for democracy and freedom of speech. Schibsted therefore sets out principles for new regulation that we believe need to be enshrined in EU law and scrutinized on national level.

1. In order to regulate social networks, **the term 'social network' must be clearly defined** on EU level. The definition could be based on existing definitions of social media or similar players. The definition should take into account the size and market share of the networks with a view to tackle the most harmful consequences for democracy.

2. In addition to defining social networks as a new category, the EU should establish a **principle of secondary liability for user-generated content** for these networks; including an obligatory notice - take down - stay down regime.

3. Furthermore, requirements for proper functionalities on the networks for **flagging illegal content** should be set.

4. In order to add clarity and transparency for the users of these networks, there needs to be an **obligation to inform users**, who have already received illegal content, that the content has been removed and why.

5. Publishers with editorial responsibility are already regulated by law and adhere to national press-ethical codes. Social networks should therefore **not modify or remove content produced under editorial responsibility** on their platform.

6. The regulation should introduce **new transparency requirements** in order for individual users to understand why they are presented with a certain type of flow of content and business users to see how their content is presented on the platform.

7. **Restrictions on freedom of speech should not be set on the EU level.** Therefore, we need a combination of EU measures and national regulation.

8. The above-mentioned proposals on secondary liability and transparency obligations of the social networks must be regulated at EU level, but **regulatory scrutiny should be left to national authorities**. In particular decisions related to content generated and uploaded by users should be taken in line with cultural differences and national rules for freedom of speech. National criminal laws in our markets already cover several harms against elections, democratic institutions, politicians and civil servants. Unfortunately, these rules are not always upheld. Member States therefore need to review their national legislation and if necessary, update it with the aim of making networks liable for the legal provisions laid down in national law. Member States should also guarantee supervision of new and existing rules.

We hope that these proposals can be taken into account in the future work of the EU Commission and want to actively participate in forthcoming discussions on these important aspects in order to ensure democracy and freedom of speech online.

2. Objective and scope

Our objective with this report is to describe our view on these matters and to propose priniciples for regulation of social networks. The aim is to reduce the negative impact for democracy and democratic institutions, without compromising the freedom of expression of citizens, or the editorial freedom of publishers.

We have consistently used the term 'social network' in this report as an alternative to the more commonly used 'social media'. The reason for this is that we want to highlight the distinction between these networks and the media with regard to publishers with editorial responsibility.

The most comprehensive categorization of problematic content conveyed through social networks that we have seen to date is found in the British Government's Online Harms White Paper, published in spring of 2019: Some of these 23 categories contribute to the undermining or weakening of democracy, while others are a threat to social norms or the well-being of individuals. In this report we do not deal with all the negative aspects of online harm. Based on our role as publishers, it is natural to focus on illegal content designed to harm democracy and democratic institutions. An additional perspective is how social networks affect journalism and the role of journalism in society.

Since we have chosen to focus on social networks in this report, search engines are excluded from the scope.

Table1: Online harms in scope

Harms with a clear definition	Harms with a less clear definition	Underage exposure to content
· Child sexual explotation and abuse. · Terrorist content and activity. · Organised immigration crime. · Modern slavery. · Eextreme pornography. · Revenge pornography. · Harassment and cyberstalking. · Hate crime. · Encouraging or assisting suicide. · Inciterment of violence. · Sale of ilegal goods/services, such as drugs and wepons (on the open internet). · Content illegaly uploaded from prisons. · Sexting of indecent images by under 18s (creating possesing, copying or distributing indecent or sexual images of children and young people under the age of 18).	· Cyberbullying and trolling. · Extremist content and activity. · Coercive behaviour. · Intimidation. · Disinformation · Violent content. · Advocacy of self-harm. · Promotion of Female Genital Mutilation (FGM).	· Children accesssing pornog raphy. · Children accesssing inappropri-ate material (including under 13s using social media and under 18s using dating apps; excessive screen time).

3. Problems that must be solved

In parallel with the positive exploitation of the opportunities networks provide, misuse has grown. Intervention in democratic elections, incitement to violence and terrorism, hate towards individuals and groups, and disinformation with the aim of destabilizing society, have become major problems.

3.1 Attacks on democratic institutions

Russian intervention on the 2016 presidential election campaign in the US and disinformation campaigns in connection with the Brexit referendum in the United Kingdom, are probably the most well-known examples of how intentional disinformation can destabilize democracy – the effects of which have not yet been adequately documented. The European Union estimates that companies connected to the Kremlin spend approximately 10 billion euros yearly on political propaganda.[1] According to experts in an EU special task group, the purpose of troll factories have never been to support specific political parties, but rather damage the overall trust in the EU as an institution. To tackle the issue Facebook established "war rooms" in Dublin and Singapore to act as a layer of defense against voter suppression, hate speech and "fake news".[2] How well the war rooms served their purpose is unclear.

Scandinavia has also been exposed to attempts to manipulate election results with the help of social networks. The proportion of "junk news" shared on social media during the 2018 Parliamentary Election in Sweden was higher than in any other European country studied, according to research from Oxford Internet Institute.[3]

During the Swedish parliamentary election in 2018, disinformation was spread via different social network channels and a particular increase in political information on Twitter was detected. The Swedish Defense Research Agency found a significant increase in Twitter bots in the months leading up to the election.[4] Six percent of all accounts were classified as bots and if accounts suspended by Twitter are included, the share of bots was 17 percent. The bot accounts are 40 percent more likely to sympathize with the right-wing populist party Sweden Democrats when compared to genuine accounts.

“Sometimes these disinformation campaigns are conducted via threats and lies being spread about individual reporters”

Photo: Randy Colas

3.2 Attacks on politicians and public employees – harmful to society
Because of their role, politicians must tolerate both just and unjust criticism more than most other people, and must also tolerate downright lies, as long as they have a fair chance to correct them and defend themselves. In recent years, we have seen organized campaigns, which are often large-scale and stem from anonymous sources, spreading personally stressful lies about individual politicians. In practice they have little opportunity to defend themselves against the lies, at least, with the same reach as the lies. This affects democracy, both because the population is misled, but also because it might lead to a silencing of politicians, or a situation where citizens are afraid to run for public office.

We have also seen examples of how individual employees in the public sector, for example, within the children’s welfare service, are personally attacked by anonymous groups, with little opportunity to defend themselves, because of the duty of confidentiality, etc.[5]

3.3 Attacks on journalism and the media
The motivation behind intentional disinformation directed at the media is often the same as attacks on formal democratic institutions – to mislead citizens in order to influence attitudes/opinions or finances in a specific way. The attacks may also be motivated by anger or discontent without any well-developed or strategic idea behind it.

Sometimes these disinformation campaigns are conducted via threats and lies being spread about individual reporters. We also see examples of actors purporting to be established media, stealing the logos and typography of the media. Undoubtedly, this erodes the trust of the media’s readers, who cannot see the difference between the original and the falsification. Eventually, social networks may become unusable as a channel for journalism.

A clear example of how a fake news source tried to spread disinformation by imitating an established paper is the Denver Guardian article from 2016.[6] The fake website created an article that was allowed to circulate on Facebook despite several media outlets´ attempts to make Facebook remove it. The article, that was designed to look like it was posted by The Denver Post, had the headline “FBI agent suspected in Hillary email leaks found dead in apparent murder-suicide.” The article spread rapidly and created a hate storm against Hillary Clinton, just days before the US Presidential Election.[7] It is impossible to know how articles like these affected the outcome of the election, but one can suspect they did

“We have probably just witnessed the beginning of deep fakes”

not benefit Clinton.

A report from The Swedish National Council for Crime Prevention studying threats and violence against occupational groups showed that journalists are particularly exposed to online threats.[8] The report states that journalists are unlikely to get support from the police or the justice system when threats are reported. Several reports from Swedish media and journalist associations indicates that women are more likely to be subject to harassment and threats.[9]

A report from Civil Rights Defenders shows that hate and threats are most often targeting individuals voicing their opinions about matters on equality, extremism and racism.[10] These topics are commonly covered by women and journalists from national minorities, hence making them more likely to be subject to hate campaigns. Not only journalists are receiving threats for practicing their profession. Influencers and social media activists belong to those who have become vulnerable in the new media landscape.

3.4 Incitement to violence

Social networks were a necessary tool for the neo-Nazis and Ku Klux Klan members for being able to mobilize during the 2017 protests in Charlottesville in order to “Unite the Right”. False information and harsh comments were allowed to flow freely on social media which caused an agitated atmosphere and violent protests. One protester was killed and 35 were injured during the aggressive protest, which was organized as a Facebook event. In the aftermath of Charlottesville, leaked documents have disclosed that Facebook (as a result of the events) is now trying to educate their moderators to be able to see the difference between opinions within the limits of freedom of speech and agitation against ethnic group.[11]

Another case where social networks have been blamed for incitement to violence is Facebook’s role in the Rohingya genocide carried out by Myanmar military in 2016 and 2017.[12] Myanmar military personnel used the social network app to mobilize an ethnic cleansing which resulted in the death of over a thousand Rohingya Muslims and forcing over half a million Rohingyas to become refugees in neighboring countries. A report by the UN has stated that Facebook’s slowness to react to this behavior contributed to the genocide.[13]

The actions taken by Myanmar military is just one of many examples of how an authoritarian government uses social networks to terrorize its own population.

3.5 Likely escalation of the problem

In the coming years, it is likely that the problems caused by the organized and massive spread of harmful lies and manipulation through social networks will escalate if countermeasures are not taken. Access to even more detailed personal data, the development of AI and more technically sophisticated possibilities for manipulation (deep fakes) are trends that threaten to further reinforce the threats to democracy.

Potentially, the development of AI will enable personal data to be processed much more efficiently, which could significantly increase the capacity to target messages more precisely than today. The possibility of influencing, for example, election results will be much higher if one reaches the right groups in the relevant constituency with disinformation containing the right messages. We have probably just witnessed the beginning of deep fakes, i.e. the manipulation of images and videos that typically give the impression of individuals saying and doing something that in reality has never happened. At present, it seems that the commonly available technical solutions for deep fakes are generally poor and therefore inauthenticity is relatively easy to detect. We must assume that this will soon change. Therefore, we are about to face a new level digital fraud which up to now has been unimaginable. In this area, we believe it is critical for both the legislator and the responsible technological environments to work proactively to ensure that we are prepared for what is most likely to happen in the future. The type of rhetoric uttered by President Trump in his attack on the media calling it the “enemy of the people”, is becoming more and more common. This may lead to a lower threshold for using instruments to influence public opinion that up to now have been considered unethical.

Photo: Rux Centea

4.
Freedom of speech under pressure

Freedom of speech is under pressure globally. It is important to recognize that regulation of social networks in many countries with weaker democratic institutions is used as a tool to curtail free speech and freedom of expression.

The international media organization, WAN-IFRA, has created a report in which they review initiatives to limit disinformation in all countries worldwide.[14] Since the term 'fake news' has been misused to characterize the type of journalism one does not like (especially by the President of the United States), the organization chooses not to use it. Nevertheless, many countries still consistently use 'fake news' in proposals for new regulatory acts.

The definitions of 'disinformation' or 'fake news' are often vague and problematic. In many cases, especially in poorly developed democracies, there is reason to fear that such legislation would prevent freedom of speech online that, according to Nordic standards for freedom of expression is fully legitimate and essential. Egypt has introduced laws against fake news without actually defining what it is, and the legislation is aimed at the users of social networks as well as the actual networks. A woman, who published a video on Facebook criticizing the escalation of sexual abuse in the country, was sentenced to two years of imprisonment, in addition to a fine. A Lebanese tourist, who posted a video reporting abuse, was jailed for eight years "… for spreading false rumors that would harm society, for attacking religion, and for public indecency." Following an appeal, the sentence was reduced to one year of imprisonment.

Several countries in Africa and Asia have set very broad and ambiguously defined limits for what one cannot spread on social networks, as such there is a high risk that free expression will be restricted. Russia has adopted two new laws, referred to as the "Law on Fake News" and "Lack of Respect for the Authorities". It is easy to envisage that both will be misused and applied to statements the Government does not like.

China passed it first regulatory legislation on social networks in 2013. Here it was established that people could be sentenced to up to seven years of imprisonment "… for posting unverified information, if it gets viewed 5000 times or shared more than 500 times. In 2016, China criminalized the production and spreading of "… rumors undermining economic and social order."

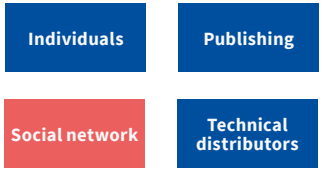
5. Nature and role of networks as channels of expression

“It is not necessarily wrong that social networks follow their own ethical guidelines on what can and cannot be published.”

5.1 Networks versus publishers
We are of the opinion that social networks should not be regulated in the same way as publishers with editorial responsibility, primarily because they do not operate publishing businesses. They neither produce nor edit journalistic content according to journalistic principles. Furthermore, publishers in Scandinavia are protected by the constitution. In Sweden there is even a specific constitutional law for publishers. This gives publishers broad regulatory freedoms, such as the right to protect their sources. This regime is complemented by press ethical principles signed by all national publishers. If social networks would be regarded as publishers, they would enjoy similar freedoms without being part of the norms-based system that in practice sets the standard for news online.

If social networks modify published material based on data they have on their users, the news feed will not be presented to them according to publishing principles, but according to community standards of the social networks. One of the well-known examples is the image of a naked girl from the Vietnam War removed by Facebook due to nudity. It is not necessarily wrong that social networks follow their own ethical guidelines on what can and cannot be published. Nevertheless, a distinction must be made between published material that has already been edited according to a set of ethical journalistic standards and other content.

5.2 Categories of mass communication actors
In our view, social networks constitute a new category of a mass communication:



Those who primarily express their opinions (individuals) and publishers, are already liable under the rules governing free expression. In most contexts, technical distributors are free of liability for the content others distribute through their networks.

Social networks differ from both the right and left sides of the model above. Generally, they do not produce their own opinions but offer technical features that allow users to design their own content. Algorithms set the terms and conditions, for example, by controlling the possibility to share and like as well as to intervene against undesirable content. The social networks differ fundamentally from the technical operators in the sense that they build algorithms that define what content each user will be exposed to. This is a form of content curation, but one that is fundamentally different from what publishers do. Social networks do not have any editorial responsibility, but neither do they provide a neutral space.

One consequence of the way the algorithms are set up is that engaging content is liked and shared to a higher degree than content, which is less engaging. In practice this means that social networks contribute to a public sphere where strong emotions are amplified and more nuanced material is downgraded. In an ecosystem where the lie travels faster than the truth, it is also extremely difficult (if not impossible) to reach all recipients of a false message with a corrected version.

6. Definitions

6.1 Definition of social networks
A precise definition of 'social network' is required to capture the special characteristics of this type of actor. Such a definition could also form the basis for assessing legal liability. The following is a selection of definitions that already exist:

"Social media are Web-based services that do not distinguish between producers and consumers of content – the content is largely user-generated – and facilitates many-to-many communication». Social media can be characterised as organised virtual communities and networks where logged in users with their own user profile can communicate with each other, with members of a self-organised group, and potentially all users of the social medium or entire Internet." (Wikipedia)

"Social media are websites and applications that facilitate content-generation, content-sharing, and participation in social networks." (Store norske leksikon (Norwegian Encyclopedia))

"… forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)." (Merriam Webster).

6.2 Definition of disinformation
In several of the initiatives that have now been adopted in Europe, i.e. in the EU Action Plan against Disinformation, the British Government's Online Harms White Paper to Parliament as well as the French Government's equivalent report, the focus is on defining and tackling disinformation as a new legal category.

The EU Code of Practice on Disinformation

The *EU Code of Practice on Disinformation* formulates a definition of disinformation and tries to use this term to describe the legal limits for legal expressions on the networks:

"As provided under the Commission's Communication, for the purpose of this Code, the Commission as well as the High Level Expert Group in its report define "Disinformation" as "verifiably false or misleading information" which, cumulatively,

(a) "Is created, presented and disseminated for economic gain or to intentionally deceive the public"; and

(b) "May cause public harm", intended as "threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security".[5]

The notion of "Disinformation" does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary, and is without prejudice to binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising."

We find the definition provided in the Code interesting, but are worried that Member States with a lower level of freedom of expression could misuse the formulation "May cause public harm", intended as "threats to democratic political and policymaking processes… " in order to stifle a healthy and critical debate well within the limits for freedom of expression as per the way the limits are set in the ECHR.

According to our legal advisers the definition could lead to conflicts about what is documentable as false or misleading. Moreover, the lawyers write: "Information must also be created, presented and spread for the purpose of gain or to mislead the public. How and by whom shall this be proved? The information must also be designed to cause public harm, including threats against democratic processes and the health, environment or security of the population without specifically defining what kind of harm is meant."

We share these concerns and believe that the formulations in the Code are imprecise and the question of proof complicated. This alone is an argument for using existing law provisions, which in Norway and Sweden at least, are far more precisely formulated.

The British Online Harms White Paper

The British Government's White Paper proposes a definition according to which disinformation is content that has intentionally been created to mislead. We are concerned that this proposal could affect the content of ordinary publishers and challenge the statutory limits for freedom of expression.

It is not sufficient for a producer of content to deliberately mislead – the definition of illegal content must also be incorporated into the regulations. The establishment of 'disinformation' as a separate category in legislation is difficult because of the definitions and problem of presenting evidence. In our opinion, it is better for legislators, at least initially, to determine the responsibility of networks for spreading content and statements that are illegal under current law.

7. Existing rules for social networks

When looking at the need to regulate social networks, it is important to understand the context they operate in and which national and EU-wide rules already exist and where there might be gaps that require new regulatory intervention. We have made an overview of these rules that social networks already should adhere to, and that should be better monitored in each Member State.

7.1 Laws and directives that set limits for interfering with the freedom of expression

At EU level, the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union protects freedom of expression. At national level, in our countries, freedom of expression is enshrined in both the Norwegian and Swedish constitutions.

This basically implies that any citizen is free to express anything, regardless of whether the statement is 'true'. The countries cannot hold a citizen legally responsible merely because the authorities define the statement as 'untrue'. These are fundamental rights in a democracy. With these overarching principles in mind, the requirement of 'truthfulness' is not a critical factor in determining whether a statement is illegal or not. It must be possible to refer to additional criteria that are clear and specific. An example of such a criterion would be specific untruthful accusations that may be defined as harmful to the affected party/parties. The principles behind freedom of speech are weighed against other fundamental rights, such as privacy and the need for the rule of law to function when setting the boundary between legal and illegal statements. The core issue is that untrue statements must have a clear, specific and severely harmful intention before it is possible to intervene.

7.2 Signals from the European Court of Human Rights (ECHR)

The ECHR has handled fives cases regarding the liability of web-based media for user-generated content since 2015. The cases are different and not all of them are relevant to the problems we are discussing here. Nevertheless, some of the signals from the ECHR are significant to the current problem.

The ECHR is concerned that strict censorship on the part of the platforms will significantly curtail freedom of speech. The reason being that networks may be overcautious in avoiding legal responsibility and consequently remove too much. In addition, the Court has focused on the difference between commercial platforms operated by highly resourceful companies and not-for-profit platforms operated by actors with few resources.

The ECHR accepts the imposition of liability on networks when the rights of individuals are severely violated. Examples are incitement to violence/ the persecution of individuals. One of the criteria for the Court is the degree to which the platform has implemented preventive measures within reasonable technical limits.

The ECHR seems to be of the opinion that 'notice and take down' should be the main rule.

Our comment to the latter is that there must be a difference between 'ongoing monitoring' and independent responsibility to remove content that is equivalent or almost equivalent to content that has already been reported and deemed illegal. We agree that the former may be inappropriate and our standpoint is that 'notice – take down – stay down' should be the main rule.

7.3 Accessorial liability and corporate punishment

From a legal point of view, the person who makes a statement is responsible for what has been expressed. If others are to be held legally responsible, the minimum requirement is that it must be authorized by law. In the Norwegian Criminal Code, so-called accessorial liability is set out in Section 15. The corresponding Swedish regulations are found in Chapter 23 of the Swedish Penal Code (swe. Brottsbalken, BrB). This is the type of accessorial liability that would typically apply to social networks.

Normally, acts that are performed before or at the same time, as the offence is committed, are punished as aiding and abetting. Passivity rarely leads to accessorial liability, however, according to the members of the legal profession from whom we have received advice, there are exceptions. The lawyers write the following "… it [is] not unreasonable to assume that when the operator of a social media platform has received positive notification of saved/published illegal content on the platform (which would normally be considered an ongoing criminal offence) the exertion of passivity after receiving such information may constitute aiding and abetting from the same point in time."

In Sweden, there is a specific - recently updated - law regulating responsibility for comments on platforms such as bulletin boards and Facebook groups. On 25 June 2019, a man was convicted in Eskilstuna District Court for failing to remove comments – deemed to be hate speech - from a Facebook group of which he was the administrator. The verdict has been appealed to Svea Court of Appeals. The law has as of yet not been applied to operators of social networks.

In general, Norwegian criminal law sets the requirement of subjective guilt in the sense that only physical persons have consciousness and as such can be held liable, not legal entities. Nevertheless, the Norwegian Criminal Code contains provisions on corporate penalties in cases when the service of an enterprise has committed a criminal act. The Swedish Penal Code has the same provisions.

We do not have an overview of how subjective guilt, accessorial liability and corporate penalties are regulated in the criminal codes of other countries. Nevertheless, with regard to the Scandinavian countries, these clarifications in legislation do not impede the accountability of social networks.

7.4 Relevant provisions in national legislation

Principally, in a situation where new legislation could lead to unintended consequences that could restrict freedom of speech in society, we believe it would be better and more precise to adapt and build on existing legislation to make networks accountable for the areas where we see most potential harm for individuals and democracy, instead of introducing new concepts.

To provide some examples, we have gone through the most relevant provisions in Norwegian and Swedish criminal law, which can be found in the Appendix.

Systematic spread of false information could potentially harm democratic processes and institutions, is not specifically covered by Norwegian legislation most probably because social networks are a relatively new phenomenon. At the same time, we see that several provisions are relevant to this topic. To clarify how the current law could be applied to social networks, it would be necessary to have a judicial review to establish whether clarifications or minor amendments to the provisions are needed in order to catch the accessorial liability of networks. In Swedish legislation, legal responsibilities for individuals are found primarily in the Penal Code, but several crimes have their own dedicated legislation (such as the Bulletin Board Law, see above). Liability for publishers and in some cases owners, printers, proliferators and authors are found in the Freedom of The Press Act (swe. Tryckfrihetsförordningen, TF).

Photo: Randy Colas

7.5 Relevant EU rules already in place

E-commerce Directive

Liability of platforms is currently mainly regulated by the e-Commerce Directive from 2000.[15] According to Article 14 in the directive, platforms can be seen as passive players that do not have any knowledge of the uploaded content and are therefore excluded from any legal liability for the content uploaded by their users. This is called the safe harbor regime. If the platform would be made aware of the content being illegal, the content has to be taken down from the platform. This is called the notice and take down procedure. According

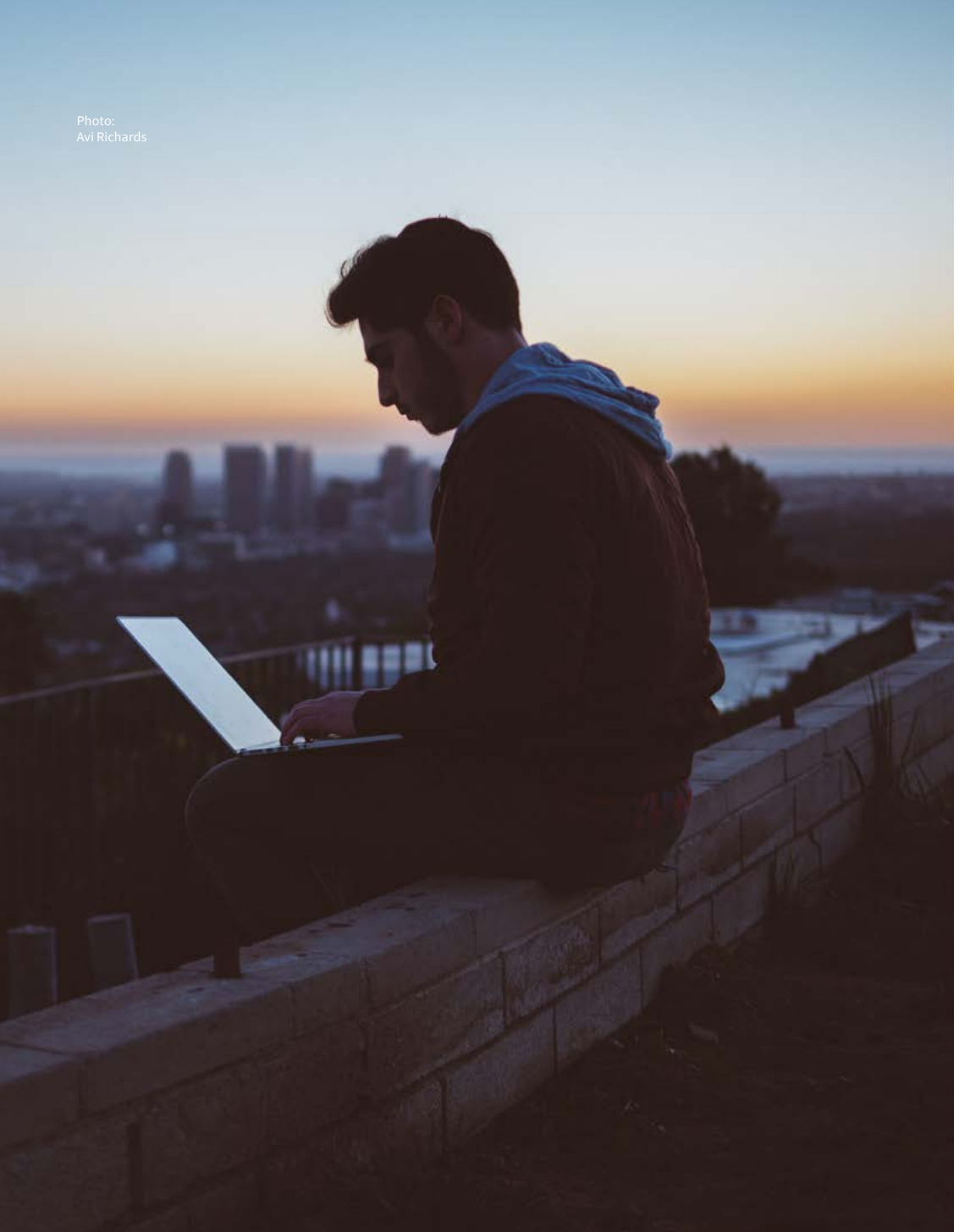


Photo:
Avi Richards

to Article 15 of the directive, platforms do not have any monitoring obligations of the content uploaded by the users. Platforms therefore have no proactive liability to monitor the platform for illegal content. Any notice has to be made either by the users or rights holders in order for platforms to take down the content.

Platforms increasingly use algorithms to recommend and prioritize content for their users. This activity indicates that platforms are aware of the nature of the uploaded content and could be regarded as active players that should have some form of liability over the content on their platforms.

This notion has sparked the need to review the safe harbor regime and the liability of platforms. Rather than an overhaul of the e-Commerce Directive, the European Commission decided during its latest mandate to introduce liability regulation for platforms in various sector-specific instruments.

The AVMS Directive

The first attempt was made in the Directive for Audiovisual Media Services (AVMS)[16] that introduced a new regulatory regime for video-sharing platforms such as Youtube and Facebook. According to Article 28 of the Directive video-sharing platforms need to take active measures in order to protect minors from harmful content, but also to take down hate speech and terrorism-related content. This directive is based on the country of origin principle, which means that the video-sharing platforms are regulated in the country of establishment. In the case of Youtube and Facebook the regulatory regime is the one of Ireland. The Directive needs to be implemented in national legislation by autumn 2020 and will be a first test bed for regulating the liability of social networks.

The Copyright Directive

The second attempt to narrow the safe harbor regime is the Directive on Copyright in the Digital Single Market[17], which introduced an article 17 that demands that active platforms need to be proactive about taking down or license copyright-protected content. This means that the liability requirement shifts from the rights holder to the platform.

In parallel the Commission issued in 2018 a Recommendation on measures to effectively tackle illegal content online, which clarifies which types of processes platforms should put in place, in order to speed up the detection and removal of illegal content. This Recommendation encourages hosting services providers to prevent the re-upload of infringing content that has already been taken down ("notice and stay down"), creating a de facto general obligation to monitor, thereby infringing Article 15 of the e-Commerce Directive.

A first concrete measure that emerged out of the recommendation is the terrorist content regulation that will require platforms to take down terrorist content within one hour of receiving notification from authorities. Companies could be fined up to 4 percent of their revenue if they consistently fail to remove terrorist content.

Although the safe harbor regime has been addressed in several sectoral instruments there is still a growing call for a need to revise the e-Commerce Directive in order to find a general liability scheme that regulates social networks and liability for all digital services in a harmonized manner. The Commission is looking at issuing an open consultation on the need to revise the e-Commerce Directive and is also thinking about issuing a new regulatory instrument that would apply to all digital services called the Digital Services Act. This new regulation is thought to upgrade liability and safety rules for digital platforms, services and products as well as address transparency issues

and enforcement of the new rules by setting up a regulatory structure either on EU level or national level.

7.6 Case law of the Court of Justice of the European Union

With regard to the limits of liability for networks in accordance with the e-Commerce Directive, one case is of particular interest at the present time: Eva Glawischnig-Pieszczek v Facebook Ireland Limited. The case concerns Facebook's responsibility for removing illegal content and the extent to which the responsibility also covers identical or equivalent content that has already been deemed illegal. The case may be of importance for the level of responsibility a network shall be ordered to take when assessing third-party content on its own initiative.

Additionally, the case also concerns how far national courts will be able to go in terms of ordering the removal of illegal content beyond their own national borders.

The case concerns a person in Austria who published defamatory comments about a politician on her Facebook page. The politician's claim that the comment was unlawful, was upheld, however, the issue was whether Facebook also had to remove identical or equivalent content to the unlawful comment.

Our lawyers wrote the following about the case processing: *"The national court initially processed the case, which was thereafter referred to the Court of Justice of the European Union with the following questions:*

– Does it comply with Article 15 of the e-Commerce Directive to order service providers to remove posts that are formulated in an identical manner as other illegal content? If so, can it also be extended to apply to other equivalent content that has been formulated differently?

Photo: Frederic Koberl

– Can national courts only order service providers to remove content within its own national borders or beyond its borders as well?"

In this context, we have not considered how justified it was to assess the original statement about the politician as unlawful in relation to the limits for freedom of expression but refer to the case since it is of fundamental importance to the interpretation of Article 15 of the e-Commerce Directive.

We assume that the ruling of the Court of Justice of the European Union in this case will also impact Germany's NetzDG, a national regulation of the responsibility of networks to remove illegal content. Here the duty to remove illegal content following a notice is limited in that networks are not required to remove republications from other sender addresses. It was supposedly done in this way in consideration of the e-Commerce Directive. From what we understand, NetzDG is in practice less effective than it would otherwise have been because of this.

The judgment of a Swedish district court in summer 2019 against the administrator of Facebook group 'Stå upp for Sverige' (Stand up for Sweden) may also be relevant in our context. The background of the case was that the defendant had received a PM containing information about some comments in the group, which the person believed were illegal and should be removed. The applicable comments were attached in a PDF. The defendant did not open the document but encouraged the sender to contact Facebook instead. The court decided that the administrator had deliberately chosen to remain uninformed about the illegal content in the group and was therefore grossly negligent. The defendant had been active in the group through posts and comments, as such the court found it unlikely that he had not seen the applicable comments.

In this case, the administrator of the group was convicted, not Facebook itself. Nevertheless, the case may be relevant to the liability of the network as an accessory to illegal acts.

8. The need for new regulation of social networks

The issue of regulating social networks and tackling disinformation has been on the political agenda in the EU and several Member States during the past years. Many national reports have proposed new rules and changes to existing legislation that include many interesting ideas.

As stated above, we are of the opinion that social networks should not be regarded as publishers and neither regulated as such. However, we are of the strong opinion that they should be made more clearly accountable under the law, by combining EU-wide rules and national legislation. In addition, social networks must clearly be made accountable for national laws.

As limits between legal and illegal speech vary between Member States, supranational regulation could be limiting freedom of speech in the most liberal countries. This would not serve us well.

At the same time, we believe that regulation would be somewhat ineffective if everything is left to the Member States. As the large social networks are global, different principles and rules in each country would in practice be impossible to apply.

We have considered whether social networks should be regulated by a voluntary, self-regulatory scheme that is not enshrined in law or whether they should be subject to ordinary legislation or a combination of both.

8.1 Ethical self-regulatory schemes
Many sectors have established self-regulatory schemes based on what is accepted and endorsed by the sector. In this instance, it is probably most relevant to look at the media sector's self-regulatory schemes. In most European countries media is regulated through various combinations of ethical codes and legislative acts. In Norway and Sweden, the media sector has adopted ethical guidelines as an addition to the constitutional legislation on the freedom of speech.

Sweden has publicly appointed a "press ombudsman" who expresses his opinions on complaints to the Swedish Press Council. The Swedish Media Association, the Swedish Union of Journalists, the Parliamentary Ombudsman and the Swedish Bar Association appoint the members of the Council. When making its assessments, the Swedish Press Council uses a code of ethics called 'Ground Rules for the Press, Radio and TV' as a basis. The Swedish Press Council can impose fees for breaching ethical standards limited to SEK 35,000 for the largest media companies.

In Norway the Norwegian Press Association, an umbrella organization for all the press organizations, including media companies with no direct membership in the organizations, appoints the members of the Norwegian Press Complaints Commission. Half of the members are appointed from the media industry and half from the general public. The Code of Ethics of the Norwegian Press set out the ethical standards and forms the basis for the Commission's decisions. The affected media, both in Sweden and Norway, are obliged to publish the Commission's decisions but i Norway there are not imposed fines.

Social networks such as Facebook and Youtube are subject to certain legislative acts but are not part of any sector-wide self-regulatory schemes. They have instead established their own community standards that guide removal of content from their platforms. These standards are developed by the companies themselves, and are not subject to any kind of sanctions.

8.2 Proposals for EU-level regulation and Member State responsibilities
In order to have a functioning system of regulating social networks we need a combination of EU measures and national regulation. We believe that the EU is best placed to regulate the liability and obligations of social networks by introducing a regulation based on general rules. This regulation would complement national laws on freedom of speech. Our proposals cover the following areas. This is a non-exhaustive list and does not go into detail:

1. Introduce a clear definition of social networks
As mentioned in paragraph 6.1, there already exists a set of definitions of social media. As we are of the opinion that networks are not media companies, we want to establish a new definition of social networks that can be based on those definitions but could also be based on the definition of video-sharing platforms in the Audiovisual Media Services Directive (AVMSD) of 2018.[18] It contains useful elements stating that these services have as essential functionality to provide "user-generated videos", that they do not have "editorial responsibility" and that the organization of the content is determined by the video-sharing provider including by automatic means or algorithms. This kind of definition could be broadened to social networks that in addition to videos also spread text and other content such as pictures and audio. We do however want to point out that the AVMSD is just a first attempt to regulate liability of content and what we are proposing for social networks is a broader set of rules for all types of social networks.
It is also important to note that the size of various social networks as well as number of members/users, is relevant

in relation to the potential harm unwanted content on the network can cause.

2. Establish secondary liability for user-generated content; including an obligatory notice - take down - stay down regime.
In order to find a balanced approach that limits harm but also protects freedom of speech, the proposal would be to introduce a requirement to immediately remove 'clearly illegal content', such as hate- and terrorism related speech within 24 hours. Any other content, where the legal nature is unclear, could be 'frozen' for up to 48 hours, in order to avoid further spread of the content.

Even though, in theory, it is possible to envisage a pre-moderation requirement for all content on social networks, it would be such an all-encompassing intervention that in reality, the nature of networks would completely change. From a freedom of expression perspective, it would be negative and set a dangerous standard. We therefore believe that intervention following a notice procedure is the most balanced regulatory measure. In order for this to work, there needs to be requirements for networks to establish efficient functionalities that enable users to easily report illegal content.

3. Set requirements for the functionality of networks so users can easily report illegal content.

4. Establish an obligation to inform users, who have already received illegal content, that the content has been removed and why.
We are of the opinion that users need to be notified when they have received illegal content in their network feed. Here one could use the analogy of the broadcast media where there is a requirement to correct any incorrect information and inform viewers of this misconduct.

5. Prevent networks from modifying or removing content produced under editorial responsibility on the platform.
More than a third of all young people in Norway use social networks as their primary news channel and 43 percent of young Swedes use Facebook as news source.[19] Almost 50 percent of the total population use networks as a news channel. This raises important questions regarding access to and the quality of news on networks.

From a Scandinavian perspective, it seems unreasonable to allow additional editing of content that publishers have already edited in accordance with ethical journalistic principles. The "Dear Mark" case originated in Norway. The editor in chief of Aftenposten newspaper reacted strongly to Facebook's refusal to publish the iconic news image of the Vietnam War showing a naked girl escaping from a napalm attack. He wrote an open letter titled "Dear Mark,'' which captured international attention.

Publishers of journalistic content adhere to national criminal law, separate legislation regulating the privileges and duties of publishers, and press-ethical codes. It is therefore important that social networks do not modify or remove published material on their platform. This would lead to double scrutiny and would go against editorial decisions. This is the same position that the *Alliance of Independent Press Councils of Europe took in 2016.*

6. Transparency requirements.
We note that public insight into the activities of networks is at present minimal. Since we deal with some of the largest companies in the world, with a formidable opportunity to impact the entire society and democracy itself, we believe this situation is unacceptable. Users of these networks are entitled to know how these actors operate their businesses. There needs to be greater insight into the use of data, such as …

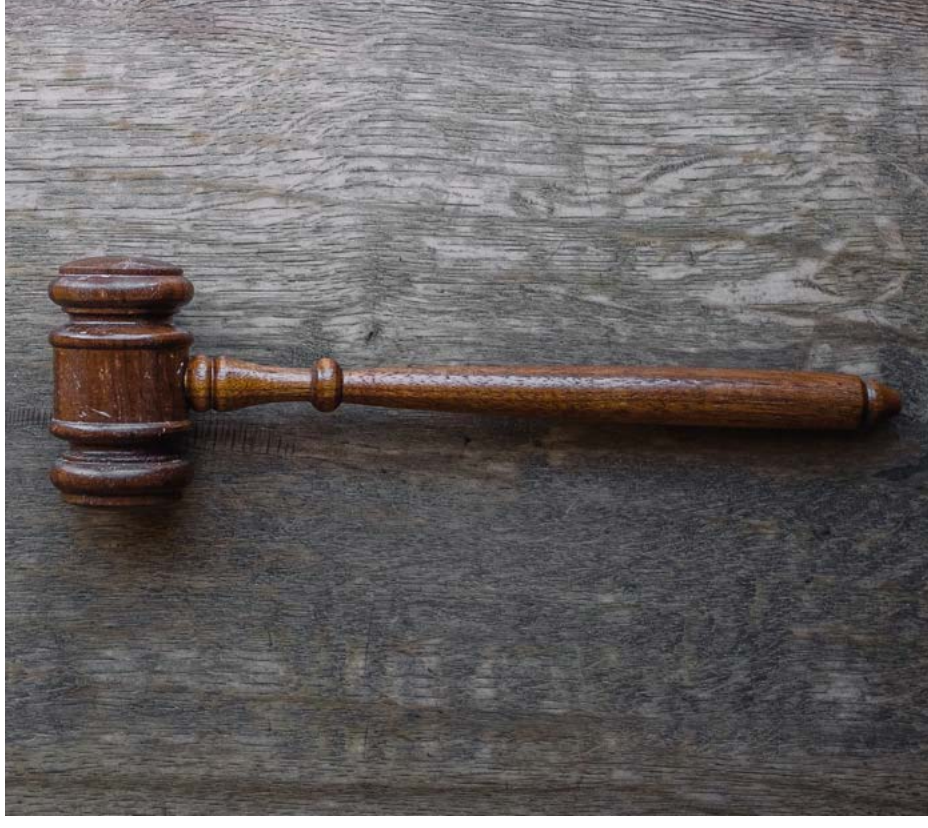


Photo:
Wesley Tingey

… the consequences of changing algorithm
… user and traffic statistics
… revenue in national markets
… the number of notices of illegal content in a given period
… how much and what content has been removed by networks

The individual users should also be able to understand why they are presented with a certain flow of content. What are the criteria that decide which content is shown and what lies behind the order of the content? We believe that there should be requirements for networks to increase the transparency of the algorithms that determine the network feed of individual users.

Similarly, we are of the opinion that business users need to understand how their uploaded content is presented on the network. It is a well-known problem that any algorithm change on the social network can have immediate and serious effects on the traffic of for example media content. Social networks will have to adopt the new Platform to Business Regulation that increases transparency between business users and online intermediary services. It is important to ensure that the regulation addresses current problems such as networks not responding to enquiries from the media industry, for example on the approval of new applications, algorithm changes, etc. If the Regulation fails to do so, it must be reviewed and revised accordingly.

7. Assign national supervisory bodies to scrutinize social networks
Schibsted wants to clearly state that limits to freedom of speech should not be set on the EU level. However, in order to ensure a harmonized system in Europe, the above mentioned overarching principles for regulation must be defined at EU level, while regulatory scrutiny must be left to national authorities. In particular decisions related to content generated and uploaded by users' decisions should be left to national authorities in line with cultural differences and national rules for freedom of speech.

National criminal law in our markets already covers several harms against elections, democratic institutions, politicians and civil servants. Unfortunately, these rules are not always upheld. National legislation therefore needs to be reviewed and if necessary updated with the aim of making networks liable for the legal provisions laid down in national criminal codes.

In particular, Member States should evaluate how existing law can be used to give social networks a clearer secondary liability in national law and if necessary, make necessary adjustments to guarantee the application. Member States should also assign supervision of these new and existing rules to suitable authorities.

In this respect, we believe that the most cost-efficient option would be to assign regulatory powers to existing supervisory bodies in the Member States. National media regulators, such as the Swedish Press and Broadcasting Authority (MPRT) and the Norwegian Media Authority are already being tasked with regulating video-sharing platforms, according to the AVMS Directive currently being implemented in national law.

Photo:
EV

Appendix

Detailing "7.4. Relevant provisions in national legislation"
Provisions of particular relevance to publishers
In Norway, the following provisions primarily regulate statements of particular relevance to publishers:

· Defamation – The Norwegian Act relating to compensation in certain circumstances, Section 3-6a
· Violation of Privacy – The Norwegian Criminal Code, Section 267
· Hate Speech – The Norwegian Criminal Code, Section 185
· Threats – The Norwegian Criminal Code, Sections 263 and 264
· Harassing Conduct – The Norwegian Criminal Code, Section 266
· Serious Stalking – The Norwegian Criminal Code, Section 266a
Excerpts from these law provisions:

Defamation has been moved from the Norwegian Criminal Code to the Act relating to compensation in certain circumstances, i.e. to civil law. Requires someone to file for a case to be tried under this provision.

Section 3-6a (compensation for defamation)
A person who negligently presents a statement designed to violate another person's sense of honour or reputation shall pay damages for the harm suffered and damages for future loss of earnings the court otherwise finds reasonable based on the exhibited guilt. He can also be ordered to pay such damages (compensation) for harm of a non-financial nature as found reasonable by the court. If the defamed person dies less than fifteen years before the defamation pursuant to subsection one takes place, his next of kin can file a compensation claim […]

There is reason to believe that networks can be made accountable as accessories for cases that fall under this provision.

Section 267. Violation of privacy
Any person who by public communication violates the privacy of another person shall be subject to a fine or imprisonment for a term not exceeding one year.

The penalty pursuant to the first paragraph does not apply to a person who has participated only through technical assistance or distribution of a magazine or periodical produced within the realm. The same applies to broadcasts. […]

An example of a violation of privacy could be the publishing of violating images and videos. The most interesting here is found in subsection two, where a person who has "participated only through technical assistance or distribution" is exempted. There is little case law here so some changes should be made to ensure that networks do not fall under the exemption.

Section 185. Hate speech
A penalty of a fine or imprisonment for a term not exceeding three years shall be applied to any person who with intent or gross negligence publicly makes a discriminatory or hateful statement. «Statement» includes the use of symbols. Any person who in the presence of others, with intent or gross negligence, makes such a statement to a person affected by it, see the second paragraph, is liable to a penalty of a fine or imprisonment for a term not exceeding one year.

«Discriminatory or hateful statement» means threatening or insulting a person or promoting hate of, persecution of or contempt for another person based on his or her
a) skin colour or national or ethnic origin,
b) religion or life stance,
c) homosexual orientation, or
d) reduced functional capacity.

This is probably relevant to making networks accountable.

Section 263. Threats
Any person who by words or conduct threatens to engage in criminal conduct under such circumstances that the threat is likely to cause serious fear shall be subject to a fine or imprisonment for a term not exceeding one year.

Section 266. Harassing conduct
Any person who by frightening or bothersome behaviour or other harassing conduct stalks a person or otherwise violates another person's peace shall be subject to a fine or imprisonment for a term not exceeding two years.

The above provisions are most relevant to Norwegian publishers. Other provisions may also be relevant to networks.

The lawyers' assessment of Sections 185, 266 and 266b:

"Social networks could be classified as accessories under Sections 185 and 266. A typical case under Section 266 is 'reckless' spreading of sexually violating images. Furthermore, Section 266 was created with 'stalking' in mind and hardly lies 'within the core area for spreading disinformation through social networks."

Attacks on democracy and democratic institutions
This is the core area of the defined scope of our work. There are law provisions here that may be relevant to the accountability of the network:

Section 115. Attack on the activities of the highest state bodies
A penalty of imprisonment for a term not exceeding 10 years shall be applied to any person who by force, threats or other illegal means puts the King, the Regent, the Government, the Parliament, the Supreme Court or the Court of Impeachment, or a member of these institutions, at risk of being hindered or affected in their activities.

The lawyers' assessment:
"It cannot be ruled out this will not affect social networks in sufficiently severe cases."

Section 117. Interference with important institutions in society
A penalty of imprisonment for a term not exceeding six years shall be applied to any person who by force, violence, threats or other unlawful and organised means interferes with the activities of important institutions in society such as a public authority, a political party or a media enterprise and thereby endangers important public interests.

These provisions have not been created to affect the problems we observe with social networks. The question is whether they could still be applied in certain situations. 'Threats' is the key term in both provisions. That being the case, the most relevant question pertaining to Section 115 is whether the threats

'affect' the activities of government agencies. We believe that such a situation can be envisioned, for example, through massive campaigns on social networks spreading threatening lies about a government institution.

The lawyers' assessment:
It cannot be ruled out that the provision may affect social works. In which case, it must be "unlawful and organized' and 'designed to endanger important public interests."

Section 131. Terrorist acts
A criminal act specified in sections 138 to 141, section 142 first paragraph, sections 143–144, 192, 238, 239, 240, 255, 257, 274, 275 and 355 is deemed to constitute a terrorist act and is punishable by imprisonment for a term not exceeding 21 years if it has been committed with terrorist intent as specified in the second paragraph.

Terrorist intent exists if an act specified in the first paragraph is committed with the intention of …
a) seriously disrupting a function of vital importance to society, such as a legislative, executive or judicial authority, energy supply, reliable supply of food or water, the banking and monetary system or medical services and disease control,
b) causing serious fear in a population, or
c) wrongfully compelling public authorities or an intergovernmental organisation to perform, submit to or omit to do something of substantial importance to the country or the organisation, or to another country or intergovernmental organization.

Any person who intends to carry out an offence as specified in the first paragraph or section 132, and who commits acts that facilitate and point towards carrying out the offence, shall be subject to punishment for attempt. An attempt is punishable by a milder penalty than is a completed violation. Section 16, second paragraph, applies correspondingly.

In this section, clause b) may be of particular interest.

The lawyers' assessment:
"This is hardly a relevant provision."

Section 136. Inciting terrorist acts; recruiting and training for terrorist acts
A penalty of imprisonment for a term not exceeding 6 years shall be applied to any person who
a) publicly incites another person to commit a criminal act specified in sections 131, 134 or 135, or sections 137 to 144, […]

Incitement to acts defined as 'terror' in the Norwegian Criminal Code is not uncommon on networks. The relevancy of this provision is whether the acts will be perceived as serious/dangerous enough for it to be applied. This may need to be investigated further.

Section 151. Purchase of votes and exercise of undue influence over voting
A penalty of a fine or imprisonment for a term not exceeding two years shall be applied to any person who in connection with a public election
a) by threats or other unlawful means seeks to influence another person's voting,

b) by providing or agreeing to provide a benefit seeks to secure another person's commitment to vote in a particular way or to abstain from voting,
c) acts in a manner that leads another person unintentionally to abstain from voting or to vote differently than intended.

This provision may be of interest even though it has not been created for the situations of concern to us. We know that false campaigns are used in connection with elections, including the Nordic countries. One question is whether such campaigns can fall under the key terms 'other unlawful means."

The lawyers' assessment:
"It cannot be ruled out that this provision may be relevant. For example, it could apply to the spread of false information about poll station opening hours."

Section 155. Violence or threats against public officials
Any person who by violence or threats induces a public official to perform or abstain from performing an official act, or seeks to achieve this, shall be subject to a penalty of a fine or imprisonment for a term not exceeding three years.

For example, there have been several cases of threats against individual child welfare employees. Such campaigns are partly organized.

Section 156. Obstruction of a public official
[…] Any person who through abusive language or other improper conduct insults a public official during or because of the performance of his/her duties shall be subject to a penalty of a fine.

Section 183. Incitement to a criminal act
Any person who publicly incites another person to commit a criminal act shall be subject to a penalty of a fine or imprisonment for a term not exceeding three years.

The probable question in this respect is how serious it will have to be before it will be considered a breach of the provision. Once again – there is hardly any case law to lean on.

Section 236. Unlawful distribution, etc. of depictions of gross violence
A penalty of a fine or imprisonment for a term not exceeding one year shall be applied to any person who with intent or gross negligence publishes or offers for sale or rental or otherwise seeks to distribute a film, videogram, etc. in which depictions of gross violence are used as entertainment in an improper manner.

The same penalty applies to any person who makes use of depictions of gross violence in a public screening, including in a television broadcast or in the transmission of such a broadcast in the realm. However, criminal liability does not extend to any person who has simply participated in the technical activities associated with the broadcast or transmission.

The provision does not apply to films and videograms that the Norwegian Media Authority has by prior review approved for screening or commercial sale. […]

The provision seems relevant, but networks need to be defined as something other than any person who has participated in "the technical activities …"

Section 263. Threats
Any person who by words or conduct threatens to engage in criminal conduct under such circumstances that the threat is likely to cause serious fear shall be subject to a fine or imprisonment for a term not exceeding one year.

In Swedish las there are corresponding rules, the Penal Code (abbr. BrB) and Freedom of the Press Act (abbr. TF) provisions. Below is a list of additional provisions which may be relevant.

TF Chapter 7, article
9 § Perverting/Obstructing the course of justice – BrB Chapter 17, article 10 §

10 § Sedition/Incitement of rebellion – BrB Chapter 18, article 1 §.
11 § Crimes against Civil Freedom (threats aimed towards interfering with the freedoms of opinion, association etc) – BrB Chapter 18, article 5 §.

References

1 Törnwall, M. (2019). Så vill Ryssland påverka valet – enligt EU-experterna. venska Dagbladet. Retrieved from https://www.svd.se/sa-vill-ryssland-styra-valet--enligt-eu-experterna

2 Kennedy, J. (2019). Dublin to be on the frontline in the war on 'fake news'. Siliconrepublic.com. Retreived from https://www.siliconrepublic.com/companies/dublin-singapore-facebook-eu-fake-news-war-rooms

3 Oxford Internet Institute, The Computational Propaganda Project. (2018). News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter. Retrieved from http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/09/Hedman-et-al-2018.pdf

4 Swedish Defence Research Agency. (2018). The Swedish election and bots on Twitter. Foi.com. Retrieved from https://www.foi.se/en/foi/news-and-pressroom/news/2018-09-12-the-swedish-election-and-bots-on-twitter.html

5 Wargeland, P. & Alnes E. (2018). Regjeringa vil straffe netthets mot offentleg tilsette. Nrk.no. Retrieved from https://www.nrk.no/norge/regjeringa-vil-straffe-netthets-mot-offentleg-tilsette-1.14319736

6 Lubbers, E. (2016). There is no such thing as the Denver Guardian, despite that Facebook post you saw. denverpost.com. Retrieved from https://www.denverpost.com/2016/11/05/there-is-no-such-thing-as-the-denver-guardian/

7 Grenoble, R. (2016). Here Are Some Of Those Fake News Stories That Mark Zuckerberg Isn't Worried About. Huffpost.com. Retrieved from https://www.huffpost.com/entry/facebook-fake-news-stories-zuckerberg_n_5829f34ee4b0c4b63b0da2ea?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAFU7ZysD4yudjTMV2pwae_uBWzi_VWkvVxSPIOsFrWJsCeIRrhzHCZg_Yg1hNZLrr0zQc6Y7O8Mtk8YUMlh5NRp64eeSZQbp-lj6Ppg_TLr6AODmGgOorLSk191v7Py10Ci1nknr6p0RF2IwTYduPJndlVKm_iaIRtXKA9tCLUj3&guccounter=2

8 The Swedish National Council for Crime Prevention (Brå). (2015). Threats and violence A report on the victimization of occupational groups important to a democratic society. Retrieved from https://www.bra.se/download/18.3f29640714dde2233b1b6b1/1434547512096/2015_Threats_and_violence_ENG.pdf

9 Haimi, R. & Sandberg, K. (2017). Sju av tio kvinnliga opinionsbildare hotas. svt.se. Retrieved from https://www.svt.se/kultur/medier/kvinnliga-opinionsbildare-utsatta-for-hot-och-trakasserier

10 Civil Rights Defenders. (2019). När samhället tystnar. En rapport om hot och hat mot oberoende opinionsbildare i det svenska civilsamhället. Crd.org. Retrieved from https://crd.org/wp-content/uploads/2019/05/N%C3%A4r-samh%C3%A4llet-tystnar-webbsidor.pdf

11 Cox, J. (2018). Leaked Documents Show Facebook's Post-Charlottesville Reckoning with American Nazis. Vice.com. Retrieved from https://www.vice.com/en_us/article/mbkbbq/facebook-charlottesville-leaked-documents-american-nazis

12 Maxur, P. (2018). A Genocide Incited on Facebook, With Posts From Myanmar's Military. nytimes.com. Retrieved from https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html?module=inline

13 Human Rights Council. (2018). Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar. Thirty-ninth session 10–28. September 2018. Agenda item 4. ohchr.org. Retrieved from https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf

14 WAN-IFRA. (2019). Public Affairs Media Policy Briefing: Tackling disinformation around the world. wan-ifra.org. Retrieved from https://www.wan-ifra.org/reports/2019/05/03/public-affairs-media-policy-briefing-tackling-disinformation-around-the-world

2019 Report

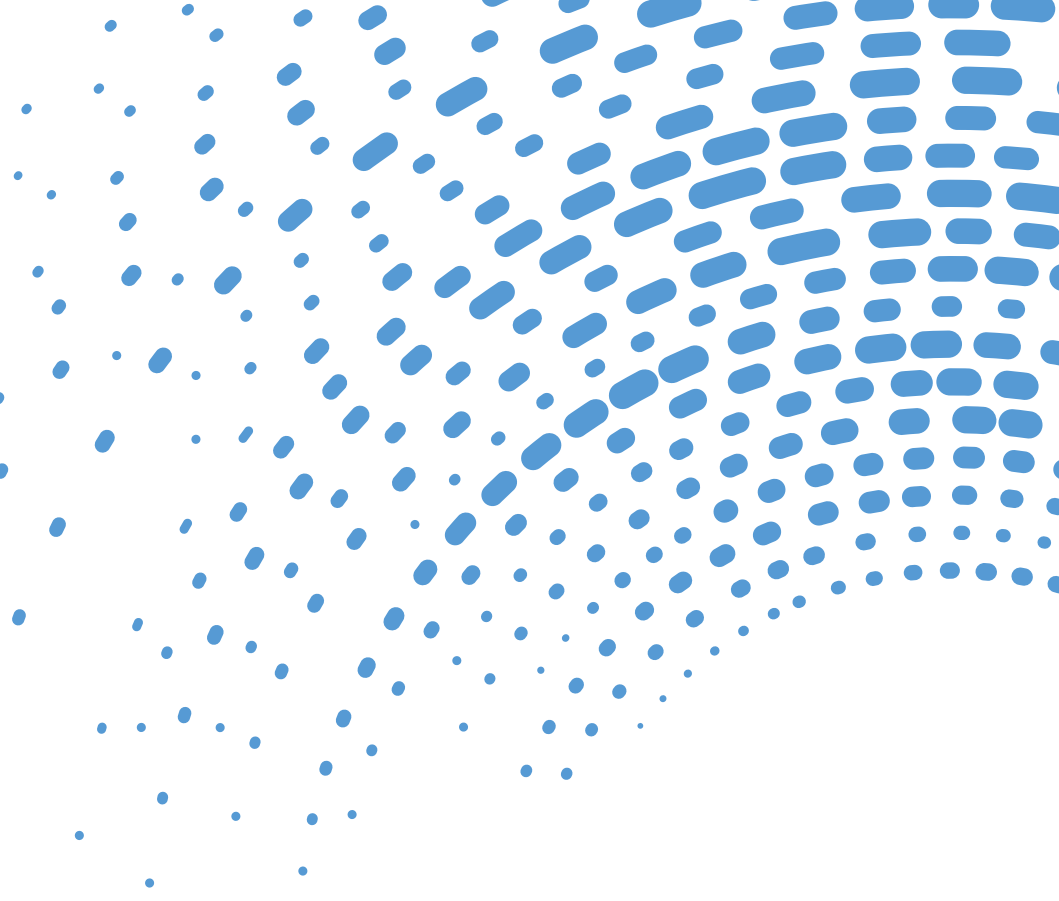
15 Directive 2000/31/EC of the European Parliament and of the Council. (8 June 2000). On certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Eur-lex.europa.eu. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

16 DIRECTIVE 2018/1808 of the European Parliament and of the Council. (14 November 2018). Amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. Eur-lex.europa.eu. Retrieved from https://eur-lex.europa.eu/eli/dir/2018/1808/oj

17 Directive 2019/790 of the European Parliament and of the Council. (17 April 2019). On copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC. Eur-lex.europa.eu. Retrieved from https://eur-lex.europa.eu/eli/dir/2019/790/oj

18 Article 1 b) aa) in the Directive DIRECTIVE (EU) 2018/1808 European Parliament and of the Council. (14 November 2018). Amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. Eur-lex.europa.eu. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&-from=EN

19 Mediebarometer. (2018). Nordicom-Sveriges Mediebarometer 2018. Nordicom.gu. Retrieved from https://www.nordicom.gu.se/sv/system/tdf/publikationer-hela-pdf/nordicom_sveriges_mediebarometer_2018.pdf?file=1&type=node&id=40345&force=0



Schibsted