Advisory Council
on International Affairs

Regulating Online Content

Towards a Recalibration of the Netherlands' Internet Policy

Advisory Report 113
24 June 2020

Advisory Council on International Affairs

The Advisory Council on International Affairs (AIV) is an independent body which advises the Dutch government and parliament on foreign policy. The AIV produces advisory reports on international affairs, both on its own initiative and on request. Its main areas of expertise are European cooperation, human rights, development cooperation and security policy. The AIV focuses on strategic dilemmas and draws attention to new policy themes with a view to the longer term. It produces independent, carefully argued advisory reports that provide analysis and interpretation of current international developments and recommendations for Dutch foreign policy, and in this way contributes to political and public debate on matters of international significance.

▸ Members of the Advisory Council on International Affairs

Chair
Professor Jaap de Hoop Scheffer

Vice-chair
Professor Joris Voorhoeve

Members
Jan Broeks Lieutenant General (ret.)
Professor Tineke Cleiren
Professor Ernst Hirsch Ballin
Professor Luuk van Middelaar
Professor Mirjam van Reisen
Koos Richelle
Monika Sie Dhian Ho

Executive secretary
Marja Kwast-van Duursen

▸ Members of the joint committee on regulating online content

Chair
Professor Tineke Cleiren

Members
Professor Edwin Bakker
Professor Janneke Gerards
Dr Bart Schermer

Executive secretaries
Robert Dekker
Dr Marenne Jansen

Trainees
Nadine Kops
Jodie in 't Groen

The AIV adopted **Regulating Online Content: Towards a Recalibration of the Netherlands' Internet Policy** (AIV advisory report 113) on 24 June 2020.

Contents

Summary 5

Recommendations 10

Chapter 1

Introduction

1.1 Focus, context and structure 14

1.2 Human rights and the internet: positive and negative aspects 15

1.3 The international arena 16

1.4 Harmful online content: what are we talking about? 21

Chapter 2

How does the internet work?

2.1 The internet is hierarchically structured: the tree metaphor 23

2.2 The roots: physical infrastructure 25

2.3 The trunk: core protocols and centralised control functions 25

2.4 The branches and the leaves: digital service providers and their applications 26

2.5 The birds: internet users 27

Chapter 3

Multilateral initiatives

3.1 The United Nations 28

3.2 The Council of Europe 30

3.3 European Union 33

Chapter 4

Complications in regulating online content

4.1 Commercialisation and the private nature of the internet 38

4.2 Jurisdiction over the internet 40

4.3 The absence of the rule of law online 41

4.4 The directive nature of technology 41

4.5 Algorithms as both catalysts of and solutions for illegal and harmful content? 42

4.6 User anonymity and responsibility 42

4.7 Inadequate national coordination 43

Chapter 5

Regulating online content: caught on the horns of a dilemma

5.1 Risks and dilemmas of active regulation 44

5.2 Risks and dilemmas of not actively regulating 45

5.3 Balancing human rights in context 46

Endnotes 50

Annexes

I Request for advice 54

II List of persons consulted 56

III List of abbreviations 58

summary

Summary

The internet has long been hailed as a forum for the free exchange of information, a promoter of human rights, emancipation, diversity and democracy, and a driver of innovation and economic growth. It is a highly prized commodity with a public core. Its open and free nature is essential. Moreover, it is an instrument that can be used to protect and promote fundamental rights and to ensure that the importance of those rights is made visible and stays visible. Partly as a result of this, the internet has acquired a central role in our day-to-day lives and in public discourse, and has rapidly developed on a large scale to become critical infrastructure in large parts of the world.

The perceived nature of the internet and its value have had an impact on the way that it has been approached, both nationally and internationally, and in both the public and private sectors. Over the past few decades, the emphasis in internet policy and regulation has been on promoting the free and open nature of the internet. In addition to this perception and appreciation, other developments and motives have also influenced regulation and policy development regarding the internet, such as economic developments (e.g. the 'new economy' of the 1990s) and political and geopolitical developments (such as globalisation and the Twitter revolutions in the Middle East).

The internet has added a fundamentally different dynamic to the dissemination of information. Content can be shared with millions of internet users all over the world within a very short time frame. Artificial intelligence and algorithms can be used to reach very precisely targeted audiences. This makes the internet a virtually irresistible instrument for political and ideological purposes. As a result, it has become increasingly clear that the internet, despite its great value, can just as easily be used to cause major harm to society. The internet can literally be used to destroy lives.

These adverse effects of the rapid development of the internet and the associated actual and potential threats to human rights have, owing to various circumstances, received relatively little attention. Governments of democratic states under the rule of law have, for a long time, prioritised the positive effects of the internet on fundamental rights, although excesses were also observed. Internet service providers (ISPs) and digital platforms were and are primarily focused on financial interests and on corresponding business models. Many users reaped the benefits of the unparalleled opportunities and were less than critical about infringements on their privacy, risks of discrimination, or the danger of their opinions being influenced.

The adverse effects of the internet are particularly apparent when it comes to the vast amounts of online content being disseminated. In this advisory report, the AIV defines 'online content' as material shared by users (individuals, groups, organisations) via the internet, such as messages posted on social media platforms, online forums and websites. Online content covers a broad spectrum of material, ranging from the clearly illegal to the completely innocent. Between these two extremes, there is content that might be considered criminal or undesirable in nature, depending on numerous social, cultural and historical factors and perceptions. Within this spectrum, this advisory report focuses specifically on the regulation of illegal, harmful or otherwise undesirable content. This concerns content that infringes on the fundamental rights of citizens or poses a threat to public values and the democratic legal order.

Regulating online content leads to difficult dilemmas. Choices have to be made all the time between different rights, including human rights, which as a result become, in a sense, diametrically opposed. On the one hand, introducing a duty of care for internet platforms, or increasing government influence on the internet, will lead to infringement on freedom of expression, the right of access to information, the right to protection of privacy and freedom of entrepreneurship. On the other hand, non-intervention could lead to discrimination, threats to security, and the undermining of other principles of democracy and the rule of law. In choosing whether to regulate and what form that should take, a balance must always be found between various rights and interests. This is a precarious process.

In choosing regulatory options, it is vital to have knowledge of and technical expertise on the internet as a global, cross-border network of networks without central governance. The same applies to knowledge of the possible consequences of certain technological interventions. A temporary, complete shutdown of the internet, to which some governments sometimes resort, may for example make it possible to block online content to a far-reaching extent, but it also instantly paralyses all of society. Targeted measures to combat specific online content being shared by individual users on internet platforms and their services are clearly less radical – but also less effective. In addition, it is necessary to take into consideration the various complications that we face due to the exceptional nature of the internet. The directive nature of the technology, the dominant position of private internet companies, the absence of the rule of law online, the fragmentary nature of existing regulations and the lack of cross-border jurisdiction make it extremely complex to address harmful online content.

Countries each follow their own path when it comes to making regulatory choices, taking into account their own views on the underlying values and interests. Countries under authoritarian rule, for example, use the internet as a government instrument to bring about social cohesion, desired behaviour, political control and national security. Other countries, including the United States, view the internet from a perspective of commercial and individual liberty. They are reluctant to employ government intervention and prefer self-regulation by tech firms. European countries, such as Germany, France and the United Kingdom, have already enacted laws to combat harmful online content, or are preparing such legislation. The European Union (EU) is also launching initiatives to combat illegal, harmful or terrorist-related online content on the internet.

Within this complex context, the Netherlands must also make choices regarding its internet policy. The Netherlands has always attached great importance to the internet as a forum for the free exchange of information, a promoter of human rights and a driver of innovation and economic growth. The Netherlands' policy has in the past been aimed at minimal regulation and a free internet market, largely in private hands. Where regulation is needed, the Netherlands has traditionally emphasised self-regulation by the tech sector itself. In light of the trends and factors described above, the AIV advocates a recalibration of this policy.

▸ Guiding principles for recalibrating internet policy

The analysis provided in this report gives rise to seven principles that the AIV believes should offer guidance for recalibrating internet policy and which form the basis for a number of more tangible recommendations.

A stronger presence of the rule of law

Viewed from the perspective of the democratic rule of law and of human rights, there is no justification for a unilateral emphasis on the importance of innovation and self-regulation by the internet sector and complete internet freedom. An effective approach to combating harmful online content will require the rule of law to have a stronger presence, in the sense that the government must ensure that the safeguards provided by the rule of law, democracy and fundamental rights are also offered where the internet is concerned. In the fight against harmful content, this means that the government must take responsibility at both national and international level. The government must engage in a political and social debate at every level to address the question of which types of content are considered acceptable in an open, democratic society governed by the rule of law and which are not, and what type of enforcement is appropriate in this context. Moreover, the government can be expected to define standards and frameworks in response to such debate, supervise enforcement of the rules that have been set and offer sufficient legal protection; all with due consideration of the basic principles of democratic state under the rule of law. For example, it would be appropriate to involve independent national expert organisations to monitor the protection of human rights. They could include national human rights institutions, ombudspersons and media authorities.

Effective national and international coordination

By now, all parties involved are becoming increasingly aware of the importance of addressing harmful online content. The nature and scope of the problems are also becoming increasingly clear – at national and international level, as well as among both public and private parties. Moreover, the activities outlined in this advisory report regarding harmful online content show that there are a growing number of initiatives and policy and regulation efforts at national and international level. At the same time, it must be noted that these initiatives and efforts take place at various, as well as between and within various sectors: national, European, international, public and private. Effective coordination and harmonisation are lacking. The immense, global and growing impact of the internet on all the people of the world – and thus the potential damage to human rights that could result from harmful online content – demands, in view of the governance and specific properties of the internet, a well-coordinated common policy shared by the various parties in the field, both public and private.

Daring to make strategic and political choices within the framework of the rule of law

Although coordination and consensus are highly important, the desire to achieve these goals must not lead to indecision. Inevitably, the reality of politics and geopolitical considerations means that strategic and political choices will have to be made that may come into conflict with the ideal solutions for dealing with harmful online content. In making those choices, the framework of the rule of law must be observed. Clear and accessible standards regarding certain forms of harmful online content exist at national and international level and are enforced by such bodies as the European Court of Human Rights. Options for action and regulation in order to deal with harmful online content must naturally remain within the boundaries defined by these international and European standards. Even where there is no clear national or international case law or legal frameworks, where consensus has not been reached, or where geopolitical interests diverge, the Netherlands must dare to make strategic and political choices that are informed by the principles of the rule of law. This holds true even if it means that the internet becomes fragmented to some extent.

Redefining the narrative: an open and free internet within the boundaries of the rule of law and fundamental rights

The dominant narrative on internet freedom is gradually evolving. Initially, the guiding principle in the Netherlands' internet policy was that the free and open nature of the internet meant that virtually any form of government regulation should be avoided. It has since become clear that internet use leads to many questions and dilemmas, and that unrestricted internet use can result in violations of other people's human rights and of the values embodied by the rule of law. It is therefore time for the Dutch government to redefine the narrative, notably by framing it as one of an open and free internet within the boundaries of the rule of law and fundamental rights. Those boundaries must apply to all parties involved in the internet, from the government to internet companies and users.

For the government, this redefined narrative provides some guidance when it comes to choosing options for taking action and regulating online content. In light of the Netherlands' perspective on human rights and the redefined narrative, less absolute and far-reaching regulatory options are an obvious choice, because these options generally have the least severe impact on human rights. That means that it is important to continue to hold to the concept that the public core of the internet must remain intact and that interventions in that area should be kept to a minimum.[1] As a result, the options for taking action can primarily be found at other levels, specifically in relation to digital service providers, applications and internet users. This means that the Netherlands must be vigilant in international discussions regarding internet technologies and standards that infringe on that public core, and that the Netherlands must adopt an active stance when it comes to technological innovations that strengthen the public core of the internet. In addition, the Netherlands must seek to implement interventions in the content layer of the internet (websites, platforms, services and their applications) that are in line with the Netherlands' firm commitment to the values of the rule of law and fundamental rights.

summary

Establishing clear frameworks around the responsibility of internet platforms

Internet platforms should take social responsibility in combating harmful and illegal content. If they must be forced to do so by means of legislation imposing a duty of care, then it is vital for that duty of care to be carefully considered. In particular, there must be clarity about what harmful content is, especially in cases where it is strongly dependent on context. However, even where clarity is lacking, internet platforms must not be permitted to shift responsibility elsewhere. In this respect, Good Samaritan clauses (which preserve exemption from liability when platforms intervene with regard to what is being posted in order to combat harmful content) could encourage internet platforms to adopt a more proactive role. It is important in this context to take undesirable side effects into account: such provisions should not give internet platforms even more control and power over the use of their platform. Finally, in defining the legal responsibility of internet platforms, it is important to take into account the nature of the service and the social position of the internet platform. In particular, parties' market power should be taken into consideration in the assessment of the nature and scope of their duty of care.

Acknowledging the importance of alternative designs for technologies and applications

Since the design of a technology or service determines the possibilities for and limitations on its use, it is important to expressly incorporate the impact that technologies and services have on human rights and social values into that design. The use of human rights impact assessments and the ethical design of systems (value-sensitive design) should be promoted. Moreover, support should be provided for the development of products, services and applications that respect public values and serve social interests (digital commons and open source). All this can help to counterbalance the dominance of commercial tech firms from other countries.

Focusing on the users

In the discussion on online content, it is important not to lose sight of users. Internet users could fall victim to harmful online content, but could also be the perpetrators. Establishing clear standards, enforcing them and raising awareness can contribute both to maintaining a healthy online environment and to protecting victims. In this context, it is also important to improve users' resilience. Education and information can help users to recognise and combat harmful content and cyberbullying and to make them more aware of privacy rules regarding the storage and use of their personal data. In addition, citizens must be enabled to take action against illegal and harmful content. This means that they should be able to report content to the internet platforms or dedicated reporting points. Finally, effective mechanisms must be put into place for private citizens to remove content, or have it removed, and to seek legal recourse against those who posted or facilitated it.

Recommendations

summary

► Recommendation 1

Recalibrate the Netherlands' internet policy

Current internet policy in the Netherlands traditionally relies heavily on self-regulation by the internet sector. This creates the risk that internet platforms will gain too much control over regulation as well as enforcement and supervision. The AIV believes that, in a democratic state under the rule of law, ultimate control should remain in public hands, particularly in a field where the private sector would otherwise dominate. Although cooperation with the private sector in multi-stakeholder governance is the preferred option, the government must have a strong presence when it comes to protecting human rights and the rule of law.

The AIV believes that efforts to combat harmful online content can only be effective in an international context. This necessitates a recalibration of the Netherlands' internet policy, shifting from self-regulation to forms of co-regulation, with an active role for the government. Such an approach must be rooted in unambiguous and coordinated national policy. This requires increasing knowledge and capacity at national level, as well as cooperation and coordination between line ministries, lower tiers of government, supervisory authorities and in parliament, in terms of both the operation of the internet and the values of democracy and the rule of law. Moreover, good national coordination is necessary (e.g. through education) to increase the resilience of the public in relation to harmful online content.

► Recommendation 2

Defend and promote the open and free nature of the internet on the basis of values of democracy and the rule of law

The open and free nature of the internet is under pressure due to attempts by countries to shield or disconnect their national part of the internet from the rest of the world. The Netherlands should focus on defending and promoting the open and free nature of the internet, but within the boundaries of the values of democracy and the rule of law (including the protection of human rights in particular). We must therefore accept that if serious threats to human rights arise or persist due to how the internet is structured, measures must be taken to protect these values. This is true even if it might lead to some regional fragmentation of the internet.

► Recommendation 3

Strengthen Dutch representation in international internet organisations

The future of the internet (its public core in any case) is determined in organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the Internet Governance Forum (IGF) and the International Telecommunication Union (ITU). The Netherlands must pursue a targeted policy to increase Dutch representation in these organisations and make people and resources available for this purpose. As one of the most important internet hubs in the world, with a well-developed internet infrastructure, the Netherlands has a good starting position in this respect.

▸ Recommendation 4

Promote the establishment of international standards for dealing with harmful online content, solidly anchored in existing human rights standards

The Netherlands should take a leading role by promoting the establishment of international standards in multi-stakeholder organisations. The Netherlands can play a meaningful role in this respect at European level (in the European Union) in particular. In concrete terms, options include initiating a European multi-stakeholder task force to identify options for regulating harmful online content. The Netherlands can also use its membership of the Council of Europe and – at a broader international level – the UN Human Rights Council to engage in international debate with like-minded countries on a human rights-based approach to online content. Existing European human rights standards, including those aimed at eradicating child pornography (the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, also known as the Lanzarote Convention) and preventing the dissemination of racist and xenophobic content through computer systems (Additional Protocol to the Convention on Cybercrime, also known as the Budapest Convention), provide guidance for the further development of international standards.

▸ Recommendation 5

Initiate measures aimed at transparency and supervision

Independent supervision of the identification and removal of harmful content by internet platforms will contribute to transparency and legal certainty for internet users. In a European context, the Netherlands should commit to the development of a European supervisory mechanism. A first step in this direction is for the Netherlands to make efforts in a European and multi-stakeholder context to provide transparency regarding the internet platforms' policies on identifying and removing harmful content. Platforms should be required to publish transparency reports that meet unambiguous criteria agreed at European level.

▸ Recommendation 6

Promote value-sensitive design and the digital commons

The actions of internet users are to a large extent determined by the scope offered to them by internet technology. That is why human rights values need to be taken into account at the very start of designing new internet technologies and applications in order to ensure that they do not have a detrimental effect on users (value-sensitive design). The Netherlands can provide funding for research programmes in this area, at European level as well as in a multi-stakeholder context. The Netherlands can also advocate European-level investment in sustainable alternatives to existing internet services that provide added value for the public (digital commons).

▸ Recommendation 7

Involve independent national expert bodies in the assessment of harmful online content

Determining whether content is illegal or harmful depends largely on the context. Independent national expert bodies could play a role in determining the criteria for assessing and removing harmful content. Examples include national human rights institutions (such as the Netherlands Institute for Human Rights), ombudspersons and independent media authorities. They could also be given an active role as trusted flaggers in monitoring the assessment and removal of harmful content in specific cases.

▸ Recommendation 8

Advocate a duty of care for internet platforms, under clear conditions

European legislation stipulates that – subject to certain conditions – internet platforms are not liable for the information that users share via the platform. Given the significant social responsibility that internet platforms have in combating harmful online content, it is important that internet platforms are given a duty of care, especially when they concern themselves with the content posed. The Netherlands must endeavour to ensure that such a duty of care is reflected in European legislation. To this end, the Netherlands must take on a pioneering role in the European debate on the role of internet platforms, more specifically in the negotiations concerning the Digital Services Act. However, a duty of care must be feasible for the platforms to implement. This requires clear criteria for assessing what constitutes harmful content, how and when content should be removed and how far a duty of care extends. These criteria can be developed and fleshed out by means of public-private partnerships, subject to the conditions defined in Recommendation 2 and with due consideration for the guiding principles defined in this advisory report. When drawing up rules on duty of care and liability, the nature, scope and market power of internet platforms should be taken into account. Undesirable side effects that could damage human rights, such as self-censorship and greater control over content, should also be explicitly taken into account.

▸ Recommendation 9

Ensure that internet platforms' terms of use are human rights-inclusive

Through their terms of use internet platforms largely determine to what extent and in which situations online content can be removed, and they currently have wide-ranging discretionary powers. In the European Union and the Council of Europe, the Netherlands must argue that internet platforms should be obliged to base their terms of use on internationally recognised human rights standards. In any case, they should endorse the UN Guiding Principles on Business and Human Rights.

▸ Recommendation 10

Increase the digital resilience of internet users

It is not always easy for internet users to recognise harmful online content or to fully comprehend the consequences of viewing or posting certain content. Through education and information, the Netherlands must invest more in citizens' digital resilience, both nationally and internationally, especially for groups that are less experienced in using the internet. In addition, they must be enabled to report harmful content and to remove it (or have it removed). A European supervisory mechanism as advocated in Recommendation 5 could play a role in this respect.

summary

Chapter 1

Introduction

The internet has long been hailed as a forum for the free exchange of information, a promoter of human rights, emancipation, diversity, and democracy and a driver of innovation and economic growth. But the internet can just as easily be used to cause major damage to society.

On the morning of Friday 15 March 2019, a 28-year-old Australian resident of the city of Dunedin, New Zealand, posted a manifesto consisting of dozens of pages on 8chan, an online discussion platform where users can anonymously exchange right-wing extremist content and child pornography. In the document he posted, the man warned that Western society and the white race were under threat from Muslim immigration. Armed with semi-automatic firearms, he then drove to the city of Christchurch. Upon arrival, he forced his way into the Al Noor mosque and began shooting attendees. He killed 44 people. Using a head camera, the shooter filmed the first 17 minutes of the attack and streamed those images via Facebook Live. In a second attack, five kilometres away at the Linwood Islamic Centre, he killed 7 more people. A total of 40 people were injured. The man was arrested 18 minutes after the first call to the emergency services.

According to Facebook,[2] fewer than 200 people were watching the livestream during the attack. None of them reported the video to Facebook. It took 12 minutes after the end of the livestream for the first report to be sent to Facebook. In response, Facebook removed the original video, but by that time it had already been viewed some 4,000 times. And by then the footage had already been shared via other platforms, such as LiveLeak, YouTube, Reddit and Twitter, and made available for downloading on various file-sharing sites. In the first 24 hours after the attack, Facebook removed some 1.5 million videos of the attack worldwide and claims to have prevented 1.2 million uploads. YouTube and Twitter also tried to remove the video, but had difficulty competing with the speed at which users shared new copies and links.[3]

The attacks prompted a great deal of response around the world. In May 2019, 18 countries (including the Netherlands), the European Commission (EC) and eight tech firms, made agreements in Paris to combat the distribution of terrorist and extremist online content. In September, another 31 countries, the Council of Europe and UNESCO joined this Christchurch Call to Action. However, the agreements made were broadly worded and voluntary. The United States claimed to support the objectives of the declaration, but did not commit itself to it, since this could be considered to be in conflict with constitutional provisions on the protection of freedom of expression.

Months later, the perpetrator's manifesto – now translated into several languages – and images of the attack can still be found on the internet.[4]

▸ 1.1 Focus, context and structure

Partly in light of the attacks in Christchurch, the Minister of Foreign Affairs asked the Advisory Council on International Affairs (AIV) to make policy recommendations for 'an approach to regulating online content that is based on the rule of law and takes an inclusive view of human rights'.

The Minister's request for advice ties in seamlessly with the question of whether the Netherlands' traditional internet policy – based on the initial optimism in the 1990s and 2000s regarding the operation and effects of the internet – is still appropriate today. No one anticipated the speed at which the internet has developed into critical infrastructure in large parts of the world and the scale at which that development has taken place, nor its disadvantageous effects as illustrated by the example given in the text box. In addition, governments and the tech sector have focused on innovation, economic development and user-friendliness; as a result, the human rights and broader geopolitical implications of the internet were long overlooked. The advantages of the internet, but also the complexity of its operations, has lulled users into complacency: in actual practice, users often seem to have very limited awareness of the threats to their privacy, of how their opinions are influenced by disinformation, or of the restrictions on access to information. This state of affairs is reflected in the limited and fragmented regulation of undesirable online content.

But the tide is slowly turning and there is a growing awareness of the darker sides of the internet. Even Facebook founder Mark Zuckerberg has been advocating legal frameworks within which harmful content can be addressed for some time now. Facebook also announced the establishment of its own independent supervisory authority in May 2020.[5] The international debate generated by such developments shows that finding solutions to address harmful online content is matter of urgency, but also that this is not a self-evident or simple process. It is within this complex context that this report must be positioned.

In this introduction, the questions posed in the request for advice are examined in more detail. The tension between the internet's importance for human rights and the risks that it poses to human rights is made visible. The introduction also describes the international arena, i.e. the context in which the issue should be placed. In addition, it defines the concept of harmful online content. Chapters 2 and 3 then respectively describe the technical workings of the internet and the current state of multilateral arrangements for regulatory cooperation. Chapter 4 discusses in more detail the limitations and preconditions specific to the internet and places them in the perspective of an effective and human rights-inclusive internet policy. Finally, the closing chapter, Chapter 5, identifies the risks and dilemmas that regulating online content poses for human rights and discusses a number of possible courses of action. This analysis culminates in the seven guiding principles laid down in the summary, which form the basis for the 10 – more tangible – recommendations made by the AIV.

▸ 1.2 Human rights and the internet: positive and negative aspects

The events in Christchurch outlined in the text box have made it painfully clear that the internet has lost its innocence. The internet can literally be used to destroy lives. Inflammatory pamphlets and images of violence are not new in themselves, nor are they necessarily connected to the internet. However, the internet has brought a fundamentally different dynamic to the dissemination of information. First and foremost, content can be shared with millions of internet users all over the world within a very short time frame. At the same time, artificial intelligence and algorithms can be used to reach very precisely targeted audiences. This makes the internet a virtually irresistible instrument for political and ideological purposes. The internet creates connections, but can also drive people apart.

These developments are not taking place in isolation. Take online disinformation campaigns used by Russian internet trolls to try and influence the US presidential elections, Islamic State (IS) propaganda videos on YouTube, Chinese coverage of matters concerning coronavirus, or coarse language on social media and in WhatsApp groups. The unclear line between openness and confidentiality of communication via the internet can entail risks to privacy. Twitter, for instance, is a public communication channel, but is used by many as if it were private communication in a group.

All these examples show that the internet can have negative effects on human rights and other public values. This has led to a growing political and social debate on whether the expression of each and every sentiment on the internet should be allowed. People are quick to look to the authorities, expecting them to put a stop to the dissemination of this type of online content by legislative means. Many also believe that tech firms (more specifically ISPs and social media platforms) should be compelled to adopt a more active duty of care when it comes to monitoring the content that users share on the internet.

The responses to the Christchurch attacks show just how much tech firms are struggling with these problems too. Despite the technological resources available to social media platforms, they are not always capable of taking effective action against harmful content posted by platform users. Governments are also still trying to find their way. Given the cross-border nature of the internet, harmful online content can only be meaningfully curbed through an international approach. However, there is a lack of international consensus on exactly what should be included in the definition of such content and what would be the appropriate way to deal with it. Perhaps even more importantly, any restriction on the free flow of information on the internet is at odds with freedom of expression and the right to information. In liberal democracies, it is precisely these vital human rights that cannot simply be curtailed.

In this international vacuum, countries each choose their own path. Countries such as Germany, France and the United Kingdom have already enacted laws to combat harmful online content, or are preparing such legislation. The EU is also launching initiatives to combat illegal, harmful or terrorist-related online content. Other countries, including the United States, are reluctant to employ government intervention and prefer self-regulation by tech firms.

> The internet connects people, but is also used to cause major damage to society.

The Netherlands has always attached great importance to the internet as a forum for the free exchange of information, a promoter of human rights protection and a driver of innovation and economic growth. The request for advice (see Annexe I) emphasises that the Netherlands' internet policy is aimed at protecting and promoting an open, free and secure internet, based on the idea that human rights are as applicable on the internet as anywhere else. At the same time, the guiding principle is that the Netherlands does not regard security and freedom as opposing concepts, but as fundamentally complementary interests. Promoting both freedom of speech and internet freedom is one of the priorities in the Netherlands' human rights policy. The government believes that universal human rights apply both offline and online. Particular attention is paid to freedom of expression, freedom to acquire information, privacy and protection of personal data.[6] Where regulating the internet is concerned, the Netherlands' policy has thus far been aimed at minimal regulation and a free internet market, largely in private hands. Where regulation is needed, the Netherlands traditionally emphasises self-regulation by the tech sector itself. This policy has long been accompanied by a low-key role for the government.

▸ 1.3 The international arena

The Minister of Foreign Affairs' request for an advisory opinion specifically concerned the regulation of online content. This makes it tempting to immediately zoom in on this specific theme. However, the subject cannot be viewed separately from the broader public debate on governance of the internet. The reason for this is that the success of measures to combat harmful online content depends heavily on the technical and organisational structure of the internet. These structures are not solely the domain of national governments, but are rather a transnational affair in which governments, companies, technical experts and civil society jointly decide on the design of the internet. This report therefore does not make a substantial distinction between domestic and foreign internet policies. For that reason, this report by the Advisory Council on International Affairs (AIV) begins by outlining the geopolitical context in which this internet governance takes place.

The growing importance of the internet

Within a few decades, the internet has grown from a boundless space in which users can freely exchange knowledge and ideas to become the backbone of international trade and global communication. In much of the world, services provided by the government and by companies are now based on information and communication technologies, including the internet. Supporting technologies such as the Internet of Things, where devices are interconnected online (examples include the smart energy meter, or an espresso machine that can be switched on via a smartphone app), have also helped the internet permeate the very fabric of society. There is great value in this respect, but it also makes societies vulnerable, especially in technologically advanced – generally Western – countries with a high internet penetration rate.[7] This certainly applies to the Netherlands, which houses a large number of data centres and is also home to the Amsterdam Internet Exchange, one of the world's largest internet hubs. A well-targeted hack could lead to major social disruption.

The internet as a geopolitical instrument

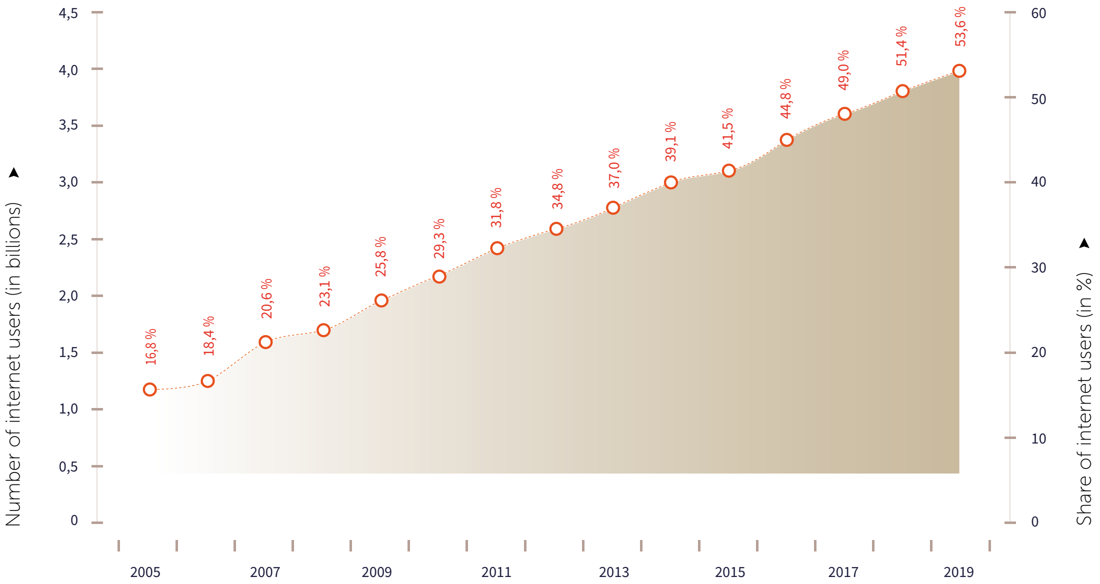
In its international strategy on cybersecurity (2017), the government wrote that various malicious actors are increasingly using the internet (the cyber domain) to pursue their own interests, for example for financial gain, the acquisition of information or politico-military purposes.[8]
The internet is increasingly being used by criminals to cause economic damage to companies, institutions and citizens, for instance by hacking, digitally holding networks to ransom and sending phishing emails. The internet has also become an attractive instrument for states to wield geopolitical power. They can use it for espionage, and disinformation campaigns in other countries can be used to disrupt political processes or pit social groups against each other. Countries such as Russia, Iran and North Korea use the internet as an instrument of hybrid warfare to destabilise other countries at relatively low cost.[9]

These developments constantly pose threats to freedom and security in society. At the same time, the decentralised, cross-border and anonymous nature of the internet makes it increasingly difficult for governments to take action against cyber aggression – from state actors as well as non-state actors. For example, investigation and intelligence services find IP addresses instead of identifiable citizens who can be prosecuted under criminal law. Classic security concepts based on national sovereignty, the deployment of military assets and allied agreements on collective defence are no longer sufficient in this new grey area. In the long term, this could even undermine the international legal order. Moreover, operations via internet often take place beyond the purview of society and the political arena. As a result – in contrast to the deployment of conventional or nuclear military assets – there is no public debate on the desirability of such actions. As long as countries do not accept responsibility for their cyber activities, it will be impossible to make international agreements and exercise mutual control over them.

Data: the new oil?

Another important development that the inventors of the internet could not have anticipated is the exponential growth in the amount of data that companies and governments collect from internet users. In political and economic terms, the possession and control of data have become invaluable.[10]
Using personal data that internet users actively relinquish (by agreeing to terms of use) or passively

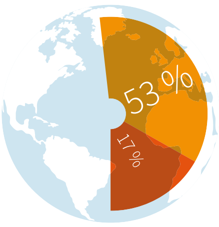
Global internet penetration rate



In 2019 an estimated 4.1 billion people used the internet, an increase of 5.3% compared to 2018.

The global internet penetration rate rose from nearly 17% in 2005 to more than 53% in 2019.

Between 2005 and 2019, the number of internet users rose by an average of 10% annually.



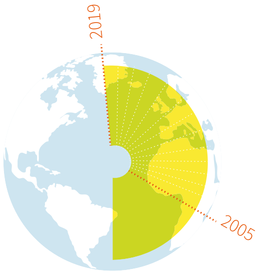


Figure 1: Global internet usage. Based on ITU, Measuring digital development. Facts and figures 2019.

deposit (by their internet behaviour), companies and governments can compile detailed profiles and use them for commercial or political purposes. This raises questions about responsibility, liability and accountability for the collection and use of data and thus, essentially, about the principles of democracy under the rule of law.

summary

> A global, harmonised and human rights-inclusive approach to online content is still a long way off.

Who controls the internet?

Because the internet has become so important, control of the international internet governance is now also an aspect of geopolitical conflict. Underlying values and interests determine how states engage with the internet and the use of data.[11] At one end of the spectrum are countries under authoritarian rule that use the internet as a government instrument to bring about social cohesion, control and national security. They fight crime and terrorism, but also political opponents, by keeping a close eye on internet users through cyber surveillance. In their view, the internet should be controlled not by private parties but by the government, and data belongs to the state. China is the most striking example of a country so strongly focused on government regulation (see also AIV advisory report 111, 'China and the Strategic Tasks for The Netherlands in Europe', 2019). At the other end of the spectrum are countries such as the United States, which view the internet from a perspective of commercial and individual freedom, while interpreting freedom of expression in near-absolute, constitutional terms. That results in minimal government regulation, private ownership of the internet infrastructure, an emphasis on innovation and commercial exploitation of personal data. In addition, the trade policies of the US government support the large US tech firms that dominate the internet. This enables them to keep newcomers out by buying up successful startups in order to neutralise potential competition, for instance. Moreover, by navigating between various national legal rules, these tech firms pay almost no taxes in the other countries where they operate.

A third model for dealing with the internet, which is positioned somewhere in the middle of the spectrum, can be found in Europe.[12] Much like the United States, Europe endorses such values as freedom of expression and online freedom of information. Private governance of the internet is considered a prerequisite for economic development and innovation. At the same time, opinions in Europe and the Netherlands seem to have shifted somewhat in the last decade, moving towards a stronger role for the government, precisely in order to be able to protect certain values of the rule of law and fundamental rights. One difference compared to the US, for example, is that there is a greater willingness in Europe to protect citizens by means of strict privacy regulations and by regulating online content. A compelling example is the General Data Protection Regulation (GDPR), with which the EU has single-handedly created a globally relevant standard. At the same time, this shows how much the European approach differs from that of China: here, great emphasis is placed on human rights such as privacy and freedom of expression when making decisions on government regulation. Moreover, unlike the US and China, Europe has virtually no major internet platforms.[13]

The above shows that different countries (and groups of countries) have adopted very different approaches to the exceptional opportunities and threats presented by the internet, determined by their culture, their own legal context, culture and underlying values. A global, harmonised and human rights-inclusive approach to online content is still a long way off.

Multi-stakeholder model

Any global governance of the internet that has been established so far has been based on what is known as the multi-stakeholder model. This means that all parties involved – businesses, governments, civil society organisations, supervisory authorities and knowledge and research institutions – work together to make joint decisions regarding the governance and development of the internet. An example is the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a private non-profit organisation that performs a number of internet-related tasks, such as assigning and specifying top-level domains, allocating domain names and distributing IP numbers (see Chapter 2). As a consequence, ICANN has a major influence on the internet's design. Also relevant are technical forums that make decisions on the technical structure of the internet, in particular the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). In addition to the technical forums, there are the more political forums such as the Internet Governance Forum (IGF) and the Global Network Initiative (GNI). While the technical forums are focused on the technical workings of the internet, the IGF and the GNI are more concerned with internet use. Nevertheless, technical aspects and usage cannot be viewed separately, since how the technology is designed determines the possibilities for its use (see Chapter 2).

The multi-stakeholder model is vulnerable. A small group of well-established experts or tech firms (supported by national governments) can exert disproportionate influence on decision-making processes. Civil society organisations are under-represented and do not have the financial means to voice strong alternative views. From a human rights perspective, the multi-stakeholder model therefore offers insufficient safeguards. At the same time, the multi-stakeholder model does offer the important safeguard that states (including countries under authoritarian rule) cannot play a dominant role in decision-making processes regarding the operation of the internet. For this reason, China, Russia and other countries[14] have, for example, already made attempts to undermine the multi-stakeholder model and give intergovernmental organisations such as the International Telecommunication Union (ITU) (and thus national governments) a greater role in decision-making processes regarding the internet. These attempts were unsuccessful, due in part to resistance from the United States, supported by the Netherlands. Nevertheless, some countries are now exerting increasing influence on the governance of the internet. This is particularly true of the United States, where much of the internet was developed and which is home to the world's largest internet companies.

As part of the broader power struggle between the two countries, China is also looking for ways to influence the governance of the internet. It is doing this, for example, by using strategic human resources policy to appoint its nationals to influential positions in international UN organisations that also play a role in the governance of the internet. Recently, the appointment of a Chinese candidate as Director-General of the World Intellectual Property Organization (WIPO) ultimately did not take place after American efforts.[15] As a member of the Security Council and as a major source of UN funding, China has considerable influence within the United Nations. In addition, China is creating an informal power base in multilateral institutions by building ties with a large number of countries, for instance by providing financial and technical support in the context of the New Silk Road. The current US administration is playing into China's hands in this regard, turning its back on multilateral cooperation and exhibiting less willingness to build international coalitions on the basis of common values. China is skilfully filling the void left by the US including in the area of internet governance.[16]

The disintegration of the global internet

The strength of the internet lies in its decentralised and cross-border nature. However, against the backdrop of the broader geopolitical power struggle on the world stage, there is a constant danger that the global internet will disintegrate into multiple regional or national internets. Russia is already working on the development of a closed internet within its own borders. China is doing something similar by not allowing access to such sites as Google, Facebook, Twitter and Wikipedia, to the benefit of Chinese government-sponsored alternatives. In this context, China is also referenced in terms of the Great Firewall, a system of internet censorship. From a human rights perspective, this disconnection of internet systems is a worrying prospect. If countries and regions lock themselves away behind digital dikes, it becomes increasingly difficult for the people living there to talk other people and exchange information, leaving little of the internet's original free and open nature intact.

> If countries and regions lock themselves away behind digital dikes, the internet loses its original freedom.

▸ 1.4 Harmful online content: what are we talking about?

In this advisory report, the AIV defines 'online content' as material placed on the internet by users (individuals, groups, organisations), such as messages posted on social media platforms, online forums and websites. Online content covers a broad spectrum of material, ranging from the clearly illegal (such as photos and videos of child abuse) to the completely innocent (such as posting holiday photos online). Between these two extremes, there is content that may be considered criminal or undesirable in nature, depending on numerous social, cultural and historical factors and perceptions. Within this spectrum, this advisory report focuses specifically on the regulation of illegal, harmful or otherwise undesirable content. This concerns content that infringes on the fundamental rights of citizens or poses a threat to public values and our democratic legal order.

Context plays an important role in assessing whether content is illegal or harmful. This context is determined by factors such as the concrete situation in which a sentiment is expressed, the sender's intent, the intended recipient, the social and political circumstances, or the juncture in time. A statement like 'I'll chop your head off' may be completely innocent within the context of two friends playing an online game, for example, but can be seen as a criminal threat if sent to a politician via Twitter. Moreover, people around the world have very different ideas about what is harmful and what is illegal; what is a mild insult to some may be seen as an actual incitement to hatred or violence by others. This makes the assessment of problematic content not only highly contextual but also, to some extent, subjective.

Since it is difficult to define in advance what is harmful or undesirable, this advisory report not only looks at the actual content and the form in which it is presented, but also at its effect, i.e. the seriousness of the infringement on collective values or human rights that results from the dissemination of the content. For example, the dissemination of discriminatory images, inflammatory language or hate speech can affect human dignity, the autonomy of individual citizens and the rights and interests of minorities or other groups in society. The functioning of society as a whole could also be disrupted when people and groups are pitted against each other. For example, the democratic state under the rule of law is threatened when online activities are used to influence how people cast their votes, or to polarise social relations. Moreover, when these activities are supported by foreign powers, national sovereignty is at stake. Finally, online content can jeopardise national and international peace and security. This could include the distribution of content with a terrorist aim, or technical or tactical instructions for committing attacks. Moreover, these effects could be very severe and direct, but may also be indirect or mild.

A statement like 'I'll chop your head off' may be innocent between two friends in an online game, but sending it to a politician on Twitter could be a criminal offence.

In summary, online content not only falls within a spectrum ranging from illegal to innocent, but can also be placed on an incremental spectrum in terms of how severely social values are violated as a result of this content. In the demand for regulation of the internet, it is always important to take this dual spectrum into account. Graphically, this can be represented as a figure plotted onto an X and Y axis.

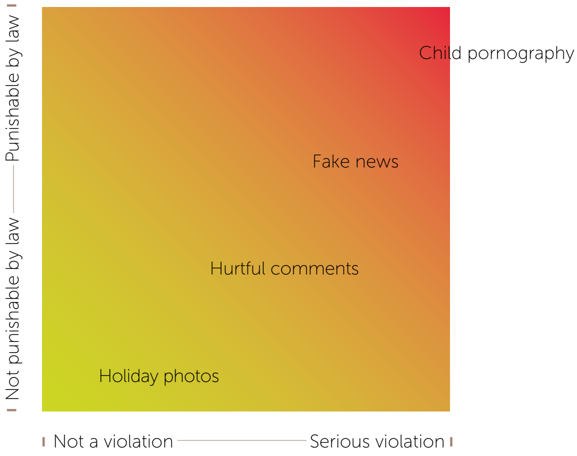


Figure 2: Spectrum of illegal and innocent content

Chapter 2

How does the internet work?

In order to be able to make considered policy recommendations for the regulation of online content, a thorough understanding of the technology behind the internet and the ecosystem of parties that play a role in creating the internet is required.

summary

Understanding the technical workings of the internet is important, because the possibilities of the technology largely determine the actions of the users. If, for example, an internet service does not offer an option to upload videos, the user will not be able to share videos via this platform. This directive definition of technology is also referred to as 'code as code' or 'code as law'.[17]

This directive effect of the technology is relevant in making regulatory choices. For example, in combating harmful online content, it may be more effective to focus on banning video upload options rather than setting up a system to monitor video content. At the same time, this also exposes the dilemmas outlined in the previous chapter: although blocking the option to upload videos may be an effective instrument, it also constitutes a significant violation of freedom of expression. The interaction between the technological possibilities and the guiding principles outlined above must therefore always be taken into account when formulating policy.

For the purpose of identifying regulatory options, it is also relevant to realise that the internet is a global, cross-border network of networks that is not under any central control. As a result, both public and private parties play a role in regulating the internet. In particular, ISPs and digital platforms (such as social media platforms) have a great deal of influence on user behaviour.

▸ 2.1 The internet is hierarchically structured: the tree metaphor

In this advisory report, the structure of the internet is visualised by using a tree metaphor.[18] This metaphor is used to offer an insight into the elementary structure of the internet, although, by its very nature, it does not correspond to all the features of the internet and the associated nuances. In this metaphor, the roots of the tree are the hard internet infrastructure (cables, routers, etc.). The trunk is formed by the core protocols – the programming language that allows computers to communicate with each other – which diverge into a number of thick branches: tech firms such as Alphabet (Google), Apple, Amazon, Facebook and Microsoft, which operate the main internet platforms. The services and applications they offer are the leaves of the tree. Around the tree, internet users circle like birds that regularly sit on the branches and leaves, making use of the various online services and applications.

In general, the lower down in the tree an intervention takes place (in the roots or trunk), the more effective the measures are to repel illegal, harmful or undesirable online content. After all, all communication in the thick branches and the crown of the tree are dependent on the roots and on transport via the trunk. However, this also means that intervention at these levels has the most far-reaching consequences from both technical and human rights perspectives. A temporary shutdown of the internet (cutting through the roots or trunk), to which some governments sometimes resort, makes it possible to block online content to a far-reaching extent. At the same time, it immediately

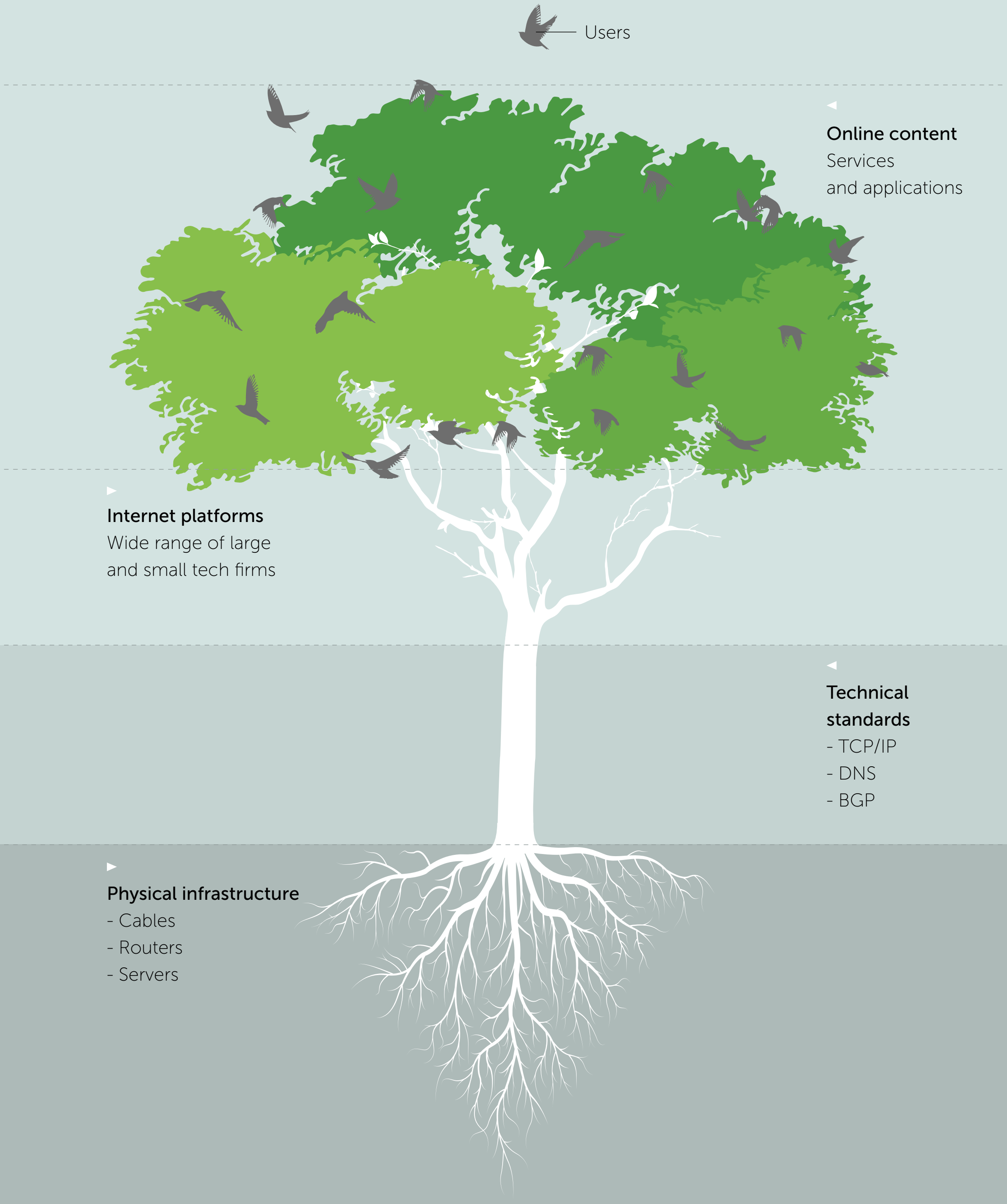


Figure 3: A metaphorical tree. Inspired by Van Dijck (2019).

instantly paralyses all of society. Targeting online content posted by individual users is less radical, but also less effective.

summary

2.2 The roots: physical infrastructure

The roots of the internet tree are the physical network infrastructure, such as the entire array of cables, routers and servers on which the internet runs. This infrastructure is, certainly in the Western world, largely in the hands of private parties such as telecom providers, hosting companies and the major tech firms. Since the networks of end users are usually not an autonomous system, they cannot simply be connected directly to the internet. To make this possible, ISPs are needed. ISPs can provide access to the internet ('access provider') or store information and make it accessible to users ('hosting provider').

2.3 The trunk: core protocols and centralised control functions

The internet is not under any central control. It has grown organically into a relatively loosely organised global network of networks that operates by using specific communication protocols.[19] Besides the protocols that enable communication via the internet, there are two control functions: numbering and the domain name system. These functions are under central control.

Communication protocols

All devices and applications connected to the internet communicate on the basis of a number of standardised communication protocols. The most important protocols are the Transmission Control Protocol (TCP), Internet Protocol (IP) and Border Gateway Protocol (BGP).

- TCP/IP
  The Transmission Control Protocol and the Internet Protocol (TCP/IP) are communication protocols used to establish reliable and robust connections between devices (nodes) that are connected to the internet.[20] This involves the use of 'packet switching'. In packet-switched networks, communications are divided into small packets that then search for the most efficient route through the network to the final destination. At the recipient's end, the individual packets are then reassembled to form the original message.[21] If there is an obstruction somewhere in the connection (e.g. because a network node fails) then TCP/IP can deliver the packets by finding a new route through the network.

- BGP
  Although the internet is a network of networks, not every network can simply connect directly to the internet. A network can only become part of the internet if it is what it known as an autonomous system. An autonomous system is a network (or networks) with a clear internal routing policy that is managed by an administrator and falls under an administrative entity (such as a company or university). This internal routing policy allows all the computers in the network to find each other and exchange information. The Border Gateway Protocol (BGP) provides the link between the autonomous systems (AS) that make up the internet. Where TCP/IP focuses on establishing connections between devices connected to the internet, BGP makes it possible to route traffic from network to network.

- Other protocols
  In addition to the protocols mentioned above, there are also more specific communication protocols running for all sorts of applications. For example, the Hypertext Transfer Protocol (HTTP) is used to send and receive web pages, the File Transfer Protocol (FTP) is used to send files and the Internet Message Access Protocol (IMAP) is used to manage email messages.

Centralised control functions

Thanks to TCP/IP and BGP, it is possible to connect computers and networks anywhere in the world without the need for central control or monitoring. This means the internet has no owner. However, in order for the internet to operate efficiently on a global scale, there are two crucial control functions that are organised centrally: numbering and domain names.

- Numbering
  For a device to be found on the internet, it needs an address: the IP address. In order to achieve uniform addressing and to prevent multiple devices from using the same address, internet addresses (IP numbers) are issued by a central body: the Internet Assigned Numbers Authority (IANA). This authority ensures that the numbers are distributed worldwide via five Regional Internet Registries. The registry for Europe, Russia and the Middle East is the RIPE Network Coordination Centre (RIPE NCC), based in the Netherlands. Together with, for instance, the Amsterdam Internet Exchange (AIE), the presence of RIPE NCC contributes to the prominent position that our country occupies internationally in the field of internet governance.[22] IANA also issues AS numbers: the numbers assigned to autonomous systems so that they can find each other.

- Domain Name System (DNS)
  Since people are not very good at remembering long strings of numbers than names, a domain name system was developed. The Domain Name System (DNS) translates alphanumeric addresses into the IP address associated with that address. IANA is tasked with maintaining the official global address book (the DNS root zone), as well as managing top-level domains such as .com, .org and .net.

- IANA
  The functions of IANA and the management of the DNS root zone are entrusted to the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN, a private non-profit organisation,[23] is therefore the most important party in the operation of the global internet. ICANN is based in the United States. ICANN has its own multi-stakeholder governance model, as discussed in Chapter I.[24] The board of directors determines the course charted by ICANN. It consists of experts representing ICANN's constituent organisations (regional registries, national registries, companies and civil society). It is striking to note that governments do not have voting rights on the board of directors. However, there is a Governmental Advisory Committee (GAC), in which 111 countries are represented. However, the GAC does not have any voting rights.

2.4 The branches and the leaves: digital service providers and their applications

Where the roots and trunk in the tree metaphor represent communication on the internet, the branches and leaves (the crown of the tree) symbolise all the websites, platforms, services and their applications. In technical terms, this level is often known as the content layer.

The major tech firms

Although the landscape of platforms and services is diverse, it can be established that the platforms and services that are most relevant to users are in the hands of a limited group of providers. They dominate the internet experience of most users. This primarily concerns the US giants (Facebook, Alphabet (Google), Apple, Amazon and Microsoft), but increasingly also includes the major tech companies based in China (such as Alibaba, Tencent, Baidu and Xiaomi).

Given the fact that these major tech firms collectively offer a huge number of platform services and applications, for the purposes of this report they can be described as the main branches of the tree, from which smaller branches and leaves sprout. This can be understood as a broader ecosystem of services and products, within which there is interaction between the services and products of a single major tech company. One example is the integration between the services and products offered by Apple: iPhones and iPads, the operating system that runs on those devices (iOS) and the applications (the App Store, Apple Music, Apple Pay) are all part of the same ecosystem.

summary

Internet platforms

Platforms, services and applications make it possible to share online content between groups of users. The business model of a digital platform consists of bringing users together. Examples could include establishing connections between holiday rental providers and tourists (Booking.com, Airbnb), or taxi drivers and passengers (Uber, Lyft). The most popular may well be the platforms that enable people to communicate with each other. In this category, there are social media platforms (Facebook, Twitter, Instagram, TikTok), video services (YouTube, Vimeo), streaming services (Twitch, Mixer), messaging services (WhatsApp, WeChat, Telegram, Signal), video conferencing services (Zoom, Starleaf, Microsoft Teams) and file transfer services (WeTransfer, Dropbox). All these services make it possible for users to share content. Although the majority of this content is benign, the platforms are also used to share illegal, harmful and undesirable content.

▸ 2.5 The birds: internet users

Lastly, the internet users can be seen as the birds flying around the tree and sometimes landing in it to use the digital platforms and online services offered via the internet. In the context of regulating online content, the users are key players. They are not only consumers of online content, but in many cases also the producers or distributors of such content, for example by creating and sharing posts and videos via these platforms. Equally relevant in regulatory affairs is the consideration that the users are not always as free as the metaphorical birds suggest. For example, the interdependence within an ecosystem created by a single tech firm may make it difficult for a user to switch to a competitor. The user's individual freedom of choice is restricted as a result.

Chapter 3

Multilateral initiatives

In order to identify options for action and regulation in Dutch policy regarding regulation of online content, it is helpful to have an overview of existing multilateral initiatives of the United Nations, the Council of Europe and the European Union. This overview offers starting points for determining courses of action for implementing regulation of online content and identifying existing initiatives for potential alignment.

▸ 3.1 The United Nations

Human Rights Council

Since 2012, the Human Rights Council of the United Nations has adopted four resolutions[25] on 'the promotion, protection and enjoyment of human rights on the Internet'.[26] The Human Rights Council emphasises in these resolutions that the rights that people have offline should also be protected online; particularly the right to freedom of expression. In that light, the Human Rights Council refers to article 19 of the Universal Declaration of Human Rights (UDHR) and to article 19 of the International Covenant on Civil and Political Rights (ICCPR).[27] The ICCPR has been ratified by 170 countries. Where the initial resolutions of the Human Rights Council primarily highlighted the positive aspects of the global and open internet, including as an instrument for developing and exercising human rights, the Council also issued a call in later resolutions to combat the negative aspects, such as advocacy of hatred, the dissemination of online information 'that may be deliberately misleading or false' and propaganda via the internet, unlawful use of personal data and online attacks on women.[28] In its resolutions, the Human Rights Council does not explicitly call for national or international regulation of online content. However, in 2018 the Human Rights Council did note that the private sector has a responsibility to respect human lives, as explained in the UN Guiding Principles on Business and Human Rights.[29]

Human Rights Committee

In 2011, the United Nations Human Rights Committee, which monitors implementation of the ICCPR by its States Parties, issued a General Comment on online freedom of expression.[30] In that document, the Committee emphasises that online content also falls under freedom of expression and that States Parties must protect the independence of online media and the ability of individuals to access such media. The same terms and conditions that article 19 of the ICCPR imposes on restrictions on freedom of expression also apply to online content. Restrictions must be specific; generic, wide-ranging bans on entire websites or platforms are in principle not permitted. Similarly, according to the General Comment, it is not permitted to ban a website or platform solely on the basis of preventing criticism of a government or a prevailing political social system.

UN Special Rapporteur on the Promotion and Protection of Freedom of Expression

The United Nations Special Rapporteur on the Promotion and Protection of Freedom of Expression, David Kaye, issued reports in 2018 and 2019 on the regulation of user-generated online content and of hate speech.[31] Both reports include specific recommendations for government authorities (states) and companies in the ICT sector.

The Special Rapporteur underlines the importance of freedom of expression as defined in the referenced provisions of the UDHR and the ICCPR. Freedom of expression is fundamental to the enjoyment of all human rights, he asserts. Governments have the obligation to facilitate and protect their citizens in exercising their right to freedom of expression. To that end, they should, among other things, promote diversity of independent media and access to information. Moreover, governments have the obligation to ensure that private enterprises do not obstruct freedom of expression.

The Special Rapporteur emphasises that freedom of expression may only be restricted in exceptional cases. These grounds for imposing restrictions, laid down in article 19, paragraph 3 of the ICCPR, are necessity to respect the rights or reputations of others, or, to protect national security, public order, or public health or morals. The Special Rapporteur also notes that article 20 (1) of the ICCPR prohibits propaganda for war and that article 20 (2) prohibits 'any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence'.[32]

The Special Rapporteur also emphasises that restrictions on freedom of expression must fulfil three conditions. First, restrictions should have a valid and sufficiently clear legal basis. That means that they are established through a sound legislative process and can be assessed by an independent judicial authority. Second, restrictions on freedom of expression must be legitimate, in the sense that it must be demonstrated that they serve to protect the interests specified in article 19 (3) or possibly article 20. Third, restrictions must be necessary and proportionate, with a view to the protection of these legitimate interests.

The Special Rapporteur believes that national regulations to combat harmful online content often do not sufficiently fulfil these conditions in practice. For instance, they rely on heavy-handed measures such as censorship or criminalisation, or prohibit content that is in fact legitimate, based on such vague terms as extremism, blasphemy, fake news and propaganda. Moreover, some laws are at odds with the right to online privacy.

The Special Rapporteur also raises questions regarding laws which are well-intentioned, but have the wrong consequences from a human rights perspective. As an example, he mentions the use of upload filters that he believes effectively lead to censorship. A second example is the notice and takedown laws in some countries, which force companies to remove harmful or illegal online content within a set time frame. The laws often lack clear criteria that can be used to establish which content is harmful or illegal, thus failing to fulfil the requirement of a valid and sufficiently clear legal basis. According to the Special Rapporteur, governments rarely make use of an independent judicial or supervisory authority and largely make internet platforms responsible for assessing which online content is unacceptable.

Internet platforms generally establish terms of use that provide rules for the posting of online content and for its removal as needed. Users must agree to these terms if they want to use a particular application or service. The Special Rapporteur notes that these terms of use are rarely based on national or international legislation on freedom of expression. As a result, internet platforms have granted themselves broad discretionary powers to determine which online content can be removed. He refers to the emergence of 'platform law in which clarity, consistency, accountability and remedy are elusive'.[33] Unclear definitions of which online content can be deleted, lack of transparency and the limited options for users to object to the removal of online content are noted by the Special Rapporteur as problematic. He advocates the inclusion of relevant human rights principles directly in terms of use, so regulation of online content by social media platforms becomes subject to the same standards that apply to restrictions on freedom of expression by governments. This means that there must be a valid and sufficiently clear legal basis, there must be a legitimate purpose, and the restrictions must be necessary and proportionate in light of that purpose.

The recommendations made by the Special Rapporteur in both reports, to governments as well as companies, aim to ensure that regulation of online content (via legislation or via terms of use) fits well within the framework of human rights and, moreover, fulfils the referenced conditions for restrictions. Governments and internet companies should, for instance, clearly describe which online content is not permitted, monitoring should only be permitted to take place after the fact, independent supervision should be provided by a judicial authority or a social media council and options should be created for internet users to lodge objections. In addition, governments and companies should be far more transparent about how regulation is designed and how it is applied in practice. Internet companies should acknowledge that international human rights standards are the basis of freedom of expression on their platforms. These companies should also endorse the *UN Guiding Principles on Business and Human Rights*.

3.2 The Council of Europe

European Court of Human Rights (ECtHR)[34]

The reports of the UN Special Rapporteur are based on multilateral treaties and conventions on human rights. At European level, those standards are given tangible form in the case law of the European Court of Human Rights (ECtHR) of the Council of Europe in particular. Countries, non-governmental organisations (NGOs), legal entities, groups and individual citizens can lodge an application with the ECtHR against one of the 47 member states of the Council of Europe, in which they can invoke the Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights (ECHR).

Freedom of expression

The right to freedom of expression is enshrined in article 10 (1) of the ECHR. The case law of the ECtHR reflects a broad interpretation of freedom of expression. For instance, such things as works of art, films, interviews and commercial information all fall within the scope of freedom of expression, as well as the ability to disseminate or receive such information. Moreover, there must be room in a democracy to express sentiments that are hurtful, shocking or disturbing. At the same time, the ECtHR has ruled that – depending on the wording used – certain racist, antisemitic or Islamophobic statements, justification of war crimes, and terrorist propaganda are not protected by article 10 of the ECHR.[35]

Like the ICCPR, the ECHR provides, in article 10 (2), for restrictions on the exercise of freedom of expression. This involves such restrictions 'as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary'. National authorities have a certain degree of freedom in assessing whether there are grounds for such restrictions. In a general sense, that freedom of assessment is more limited proportionate to the significance of the statement in question in discussions regarding democracy and the rule of law, or if it is relevant to matters in the general interest. In those cases, there must be compelling arguments and the measures must be equipped with appropriate safeguards. In such cases, the ECtHR carefully assesses whether freedom of expression has not been restricted more radically than was strictly necessary to achieve a compelling aim and whether there is a reasonable balance between the importance of that aim and the right that has been infringed by the restriction.

In contrast to the recommendations of the UN Special Rapporteur, according to the ECtHR a ban on the dissemination or publication of certain content before it actually takes place is not by definition prohibited. However, since freedom of expression is a fundamental and essential right in a democratic society, states do have a minimal freedom of assessment in this respect. Again, the ECtHR carefully assesses whether the prior restrictions were necessary and proportionate to the pressing objectives in the general interest.

This shows that the ECtHR, too, uses three criteria to determine whether a restriction on freedom of expression is permitted, which correspond to a significant extent to the conditions discussed above in the UN context:

1. Prescribed by law: according to the ECtHR any restriction must be accessible and foreseeable, so citizens know where they stand.
2. Legitimate aim: it must be demonstrated that the restriction pursues one of the aims listed in article 10 (2) of the ECHR.
3. Necessary in a democratic society (necessary and proportionate): the restriction must be necessary to achieve the stated aim, a 'pressing social need'; the reasons given for the restriction must be relevant and sufficient; and there must be a reasonable balance between the aim pursued and the infringed right.

Internet platforms and other internet intermediaries

In various judgments, the ECtHR has held that content posted on social media and other digital platforms also falls within the scope of article 10 of the ECHR. After all, these platforms make it possible to exchange information and ideas and offer a forum for transmitting and receiving information from others, or creating and sharing information within a group.[36] Under the ECHR, internet platforms cannot be directly held to account for content posted on their forums or platforms: applications can be lodged with the ECtHR against the state only. However, the ECtHR has ruled that it is not incompatible with freedom of expression for a domestic court to hold an internet platform liable for placing or not removing online content on the platform if it is clearly illegal, as may be the case with hate speech and incitement to violence. In that case, the platform can reasonably be required at national level to remove the content. In considering such cases, the ECtHR looks at issues such as the context in which a statement is expressed, the nature and possible consequences of the comments, the measures already taken by the platform itself to remove the content, the possibility of holding the original authors liable and the consequences for the platform of not removing the content.[37] The ECtHR has acknowledged that requiring an internet platform to remove unlawful content itself may result in these platforms automatically filtering online content, for example using algorithms. Unlike the UN Special Rapporteur, the ECtHR is not necessarily opposed to that, since it may be the only way to protect the legitimate interests and rights of others from unlawful content.

Relevant treaties and conventions of the Council of Europe

In October 2007, the member states of the Council of Europe concluded the Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, also known as the Lanzarote Convention, which entered into force in the European part of the Kingdom of the Netherlands on 1 July 2010.[38] The establishment of the Lanzarote Convention was a direct consequence of the increasing use of the internet by both children and perpetrators, as a result of which child pornography could easily be disseminated across national borders and on an increasingly large scale. The States Parties to the Convention seek closer cooperation to prevent and combat child sexual abuse.

The Lanzarote Convention offers guidance on regulating online content because it provides definitions, for issues such as sexual abuse, child prostitution and child pornography, that have been agreed in a broad-based European context. The Convention also provides an overview of relevant criminal offences. For instance, it requires criminalisation of production, dissemination, acquisition and accessing of child pornography by means of ICT.

In early 2003, the member states of the Council of Europe adopted an Additional Protocol to the Convention on Cybercrime (the Budapest Convention, 2001), which entered into force in the

Kingdom of the Netherlands on 1 November 2010.[39] The signatory states to this Additional Protocol[40] undertake to adopt national legislation to establish the distribution or otherwise making available of racist and xenophobic material to the public through a computer system as a criminal offence, 'when committed intentionally and without right', as well as racist and xenophobic motivated threats and insults, and denial, gross minimisation, approval or justification of genocide or crimes against humanity.

In accepting the protocol, the following statement was made on behalf of the Kingdom of the Netherlands, as follows: 'The Kingdom of the Netherlands will comply with the obligation to criminalise the denial, gross minimisation, approval or justification of genocide or crimes against humanity laid down in Article 6, paragraph 1, of the Protocol where such conduct incites hatred, discrimination or violence on the grounds of race or religion'. Another example of existing European human rights standards on combating the dissemination of racist and xenophobic content can be found in article 19 (1) of the European Social Charter, which calls on states to take all appropriate steps against misleading propaganda and false information relating to emigration and immigration.

Committee of Ministers

Since the 1950s, the Committee of Ministers of the Council of Europe has established an extensive system of (non-binding) recommendations, declarations and resolutions regarding media and the information society.[41] In 1997, the Committee adopted a recommendation on 'the gratuitous portrayal of violence in the various electronic media at national and transfrontier level',[42] which also mentioned the role of the internet. Since then, the Committee has repeatedly expressed positions on issues such as regulating the internet and online content, human rights of internet users, and the roles and responsibilities of internet intermediaries.[43] For this advisory report, it is mainly relevant to note that the Committee of Ministers follows the case law of the ECtHR and assigns a central position to freedom of expression and the right of internet users to search for, receive and communicate any information and ideas they wish. The Committee follows the reasoning of the ECtHR that online content falls within the scope of article 10 of the ECHR and that governments can, in accordance with the conditions laid down in article 10 (2) of the ECHR, impose restrictions on online content that incites discrimination, hatred or violence. In a number of areas, the Committee also offers tangible starting points that had not yet been expressed so clearly in the case law of the ECtHR. For instance, the Committee has stated that internet users must be able to choose not to disclose their identity on the internet, but that they must take account of the fact that national authorities may take measures that lead to their identity being revealed, for instance for the purposes of combating crime.

The Committee believes that human rights and the standards associated with those rights take precedence over the general terms and conditions formulated by internet companies, to which internet users must consent in order to use certain services or applications. At the same time, the Committee believes that it is acceptable for internet providers and parties offering online services to restrict certain content, on the basis of their own policies. In doing so, they must specifically describe what they consider unlawful or inappropriate content and how they deal with such content. They must also ensure complaints procedures are in place.

With regard to internet intermediaries, the Committee of Ministers has recommended that they cannot be held liable for content posted by third parties if the intermediary only transmits or stores the content. However, if the internet intermediary plays a larger role and, for instance, produces or curates content itself, they can be held liable for illegal content. In that case, the intermediary bears a greater responsibility for removing such content. The Committee has called on the member states of the Council of Europe to work in concert with the internet sector in order to develop a system of self-regulation or co-regulation of online content, based on the requirements of lawfulness, necessity and proportionality. Internet companies should also follow the UN Guiding Principles on Business and Human Rights.

3.3 European Union

The European Union has various instruments at its disposal that are relevant in combating harmful online content. The human rights framework for these instruments is provided by the Charter of Fundamental Rights of the European Union. Relevant parts of the Charter include not only freedom of expression and information (article 11) and freedom of the arts and sciences (article 13), but also the call for non-discrimination (article 21) and protection of the rights of the child (article 24). Although the Charter as drafted in 2000 is one of the most recent documents on fundamental rights, it could not take into account how the internet would develop in this century. At the invitation of the ZEIT-Stiftung Ebelin und Gerd Bucerius foundation, a group of experts has developed a proposal for a Charter of Fundamental Digital Rights of the European Union,[44] which would not be legally binding in the same way as the Charter of Fundamental Rights but could serve as a guideline for the development of the law in this field.

In its policy on this subject, the EU seems torn between two lines of thinking. On the one hand, EU policy is aimed at ensuring internet intermediaries embrace their social responsibility by proactively taking steps to combat the dissemination of harmful and illegal online content. On the other hand, the EU does not want to hold these intermediaries liable if such content is shared via their platforms.[45]

> EU policy is aimed at ensuring internet intermediaries take steps to combat the dissemination of harmful and illegal online content. However, the EU does not want to hold these intermediaries liable if such content is shared via their platforms.

As a result, the EU has opted for a separate strategy for dealing with the dissemination of three different types of harmful content: illegal online content (including hate speech), online content of a terrorist nature and online disinformation. A number of these instruments are legally binding, while others are primarily intended to promote voluntary self-regulation by internet platforms. In addition, in February 2020 the European Commission published a White Paper on Artificial Intelligence[46] and a Communication on a European data strategy, in which further policy proposals were announced.[47]

EU legislation

Electronic Commerce Directive

In June 2000 the European Parliament and the Council of the European Union adopted the Electronic Commerce Directive.[48] This Directive stipulates that an internet service provider or internet service that transmits or stores user information is not liable for the content of that information if a number of conditions have been met. Access providers are exempt from liability if they do not take the initiative to transmit the information, do not determine the recipients and do not select or change the information. If these conditions are met, the providers are considered a mere conduit and are not liable.

A hosting provider is not liable for the information stored on its servers if it is not aware of the unlawful nature of the information and cannot reasonably be required to know. If the provider is aware of the information (e.g. because it has been notified), the provider must immediately remove the unlawful information or make it inaccessible. This liability exemption for hosting providers is relevant because internet platforms also fall within the scope of this provision, and can therefore invoke the exemption.

The Electronic Commerce Directive also states that member states may not impose a general obligation on internet services to monitor the information they transmit or store, nor to actively 'seek facts or circumstances indicating illegal activity'.[49] These EU rules on liability of internet services are in line with the recommendations of the Committee of Ministers of the Council of Europe in this regard.

The Electronic Commerce Directive also enables member states to impose restrictions on information services. Such measures must be necessary for the protection of public policy, including the protection of minors, the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons. Protection of public health, public security and consumers are also valid reasons for restrictions.

Audiovisual Media Services Directive

The provisions regarding liability outlined above are also part of the Audiovisual Media Services Directive (2010).[50] In the 2018 revision of the Directive, video platform services were added to its scope.[51] This includes such platforms as Netflix and YouTube, as well as Facebook when videos are shared on that platform. The Directive also provides for restrictions to be imposed on audiovisual media services, similarly to the relevant provisions in the Electronic Commerce Directive.[52]

Other legislation

The Council Framework Decision of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law requires member states to criminalise these acts. It concerns public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, colour, descent, religion or belief, or national or ethnic origin; the above-mentioned offence when carried out by the public dissemination or distribution of tracts, pictures or other material; and publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes. Article 9 of the Framework Decision stipulates that each member state must ensure that its jurisdiction extends to cases in which the conduct was committed through an information system and the offender or the information system is in its territory.[53] The Directive of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography[54] and the Directive of 15 March 2017 on combating terrorism[55] respectively prohibit the distribution, dissemination or broadcast, online or offline, of child pornography and of materials that incite the commission of terrorist offences.

Code of Conduct on online hate speech

In May 2016, the European Commission reached agreement with Facebook, Microsoft, Twitter and YouTube on a Code of Conduct on countering illegal hate speech online.[56] In 2018, Instagram, Google+, Snapchat and Dailymotion also endorsed this Code of Conduct. The Code of Conduct states that the majority of valid notifications concerning hate speech should be assessed within 24 hours and the content removed from the platform if necessary. The platforms themselves determine on the basis of their terms of use whether there is cause for removal. The Code of Conduct defines content containing hate speech as content that incites hatred or violence against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin.[57] The platforms also promise to invest in promoting awareness among internet users regarding what kind of content is not permitted.

The Code of Conduct on countering illegal hate speech online is not legally binding, but is a form of self-regulation by internet platforms. In these efforts, they work with a network of 'trusted flaggers'. These organisations and civil society initiatives flag potentially illegal content on the platforms on the basis of their expertise. According to the European Commission, these internet platforms managed to assess 40% of hate speech notifications within 24 hours in 2016. In 2019, that figure was 89%. The amount of content that was subsequently removed rose from 28% in 2016 to 72% in 2019.

The progress report published by the Commission does not address the objectives for raising awareness as laid down in the Code of Conduct, so it is unclear how those objectives are being pursued and to what extent they are being achieved.[58]

Communication on illegal online content

In September 2017 the European Commission published a Communication on tackling illegal content online.[59] The European Commission states in the Communication that what is illegal in the physical world is also illegal online. This includes incitement to terrorism or hatred, as well as child sexual abuse material. The EC believes that online platforms have an important social responsibility to protect internet users and all of society from these things. At the same time, the European Commission notes that taking voluntary, proactive steps does not automatically lead an online platform to lose the benefit of the liability exemption provided for in the Electronic Commerce Directive, as discussed above.

In the Communication, the European Commission also provides several guidelines and principles for internet platforms to combat the dissemination of illegal content more effectively in cooperation with national authorities in the member states. In addition, online platforms must explain their content policy in an understandable way in their terms of use and publish transparency reports on the nature of the notifications received and the actions taken. In order to prevent excessive removal of online content, the platforms must set up clear objection procedures.

This Communication was followed in March 2018 by a – non-binding – Commission Recommendation on measures to effectively tackle illegal content online,[60] in which the guidelines mentioned above were fleshed out into operational measures that the member states and internet platforms should take in order to identify and remove illegal content.

Proposed Regulation on online terrorist content

In 2018 the European Commission presented a proposal for a Regulation on preventing the dissemination of terrorist content online.[61] The European Parliament adopted the proposal for the Regulation in April 2019; it is currently being negotiated by the member states. This proposal concerns providers of hosting services and aims to introduce a number of new measures. For example, the competent bodies and judicial authorities in a member state should be able to order a provider to remove illegal online terrorist content within one hour.The proposal also harmonises the minimum requirements that hosting service providers must take into consideration in assessing online content of a potentially terrorist nature.[62] In certain cases, providers will also be subject to a duty of care to proactively take 'appropriate, reasonable and proportionate actions'[63] to combat terrorist online content on their services. At the same time, this proposal states that the Regulation must not diminish the — conditional – liability exemption laid down in the Electronic Commerce Directive.[64] To prevent wrongful removal of legal online content, hosting service providers must have, for example, a complaints procedure in place and publish an annual report on the measures they have taken.

Policy measures on online disinformation

The EU has adopted various policy measures to combat online disinformation. In a Communication in April 2018, the European Commission described disinformation as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm'.[65] The European Commission proposed the following measures to tackle online disinformation:[66]

- Adopting a code of practice for internet platforms.
- Creating an independent European network of fact-checkers.
- Launching a European online platform with access to EU-wide open data on disinformation to support the network of fact-checkers.
- Supporting member states in ensuring that their elections are resistant to increasingly complex cyber threats, including online disinformation and cyberattacks.
- Fostering awareness among internet users (media literacy).
- Encouraging voluntary online identification in order to improve the traceability of information providers.
- Promoting quality journalism to ensure 'a pluralistic and diverse media environment'.
- Establishing a coordinated European strategic communication policy.

In October 2018 Facebook, Google, Twitter, Mozilla, industry bodies from the advertising sector and advertisers signed the EU Code of Practice on Disinformation.[67] In May 2019 Microsoft also signed it.[68] This Code of Practice contains a large number of agreements to tackle disinformation – online – including providing more transparency about political advertising, closing fake accounts, working with fact-checkers and improving the visibility of information that has been fact-checked. Although in the above-mentioned Communication the European Commission also sought to achieve greater transparency regarding how algorithms work and are monitored by third parties, this aspect is barely addressed in the Code of Practice.

In two reports on compliance with this Code of Practice, the Commission concluded that the Code is a good instrument for dialogue with internet platforms and that it has improved the platforms' transparency regarding their policies on disinformation. At the same time, the Commission believes that cooperation with fact-checkers could be improved and that platforms should provide access to more data for scientific research. These reports also indicate that the commitments to increase awareness of disinformation among internet users have not yet been sufficiently fleshed out.[69]

The Code of Practice is one of the elements mentioned in the European Action Plan against Disinformation[70] presented in December 2018 by the European Commission and the High Representative for Foreign Affairs and Security Policy. The aim of this action plan is to reinforce the capacity of the EU institutions and coordination between member states to identify and counter the use of disinformation by actors within the European Union and from third countries. In line with the Communication from the European Commission on this matter, the action plan will also seek to improve public awareness.

European data strategy

In February 2020, the new European Commission presented its plans for a European data strategy.[71] The strategy is focused on transforming Europe into a leading data-driven society. From the perspective of content regulation, two elements from the data strategy are relevant. These are: 1) revising the rules for liability of internet intermediaries and 2) the rules for the use of artificial intelligence.

Revised liability rules for internet intermediaries

Ursula von der Leyen, President of the European Commission, explained in her Political Guidelines that she wants to upgrade the existing rules on liability.[72] To that end, the Electronic Commerce Directive will be replaced by a Digital Services Act. Although no concrete proposals had been published at the time of writing, the general expectation is that there will be a stricter liability regime for internet intermediaries, with a focus on the duty of care those internet intermediaries have.[73]

Rules for the use of artificial intelligence

The European Commission also wants to formulate rules for the application of artificial intelligence. To that end, the European Commission has published a White Paper on the use of artificial intelligence.[74] The White Paper underlines the importance of transparency and explainability of algorithmic decision-making and builds on the EU High-Level Expert Group on Artificial Intelligence's Ethics Guidelines for Trustworthy AI.[75]

Chapter 4

Complications in regulating online content

Effective and human rights-inclusive regulation of harmful online content is complex. Pressing issues include commercialisation, the lack of jurisdiction, the absence of the rule of law online, the directive nature of technology, the use of algorithms, the anonymity of users and the lack of comprehensive coordination.

▸ 4.1 Commercialisation and the private nature of the internet

Since the 1970s, the internet has been developed by publicly funded US government bodies and research institutions. The technology experts involved were generally motivated by idealism; when they built the internet, they were aiming to create a free haven for ideas and knowledge exchange without government interference. Accordingly, knowledge of the technology and protocols of the internet was available to everyone. From the 1980s, the rest of the world began to be connected to the internet. The invention of the World Wide Web subsequently made the internet easily accessible to the public, causing it to grow enormously from the early 1990s on. That growth also marked the start of the commercialisation of the internet. In actual practice, the concept of an open, free internet turned into the idea that internet services and online information should be freely accessible. However, it turned out that this required advertising in combination with the collection of internet users' data in order to be economically feasible. As discussed in Chapter 2, as a consequence of this business model, several major tech firms emerged that have since come to dominate the internet.

The mission statements of the dominant tech firms are generally idealistically formulated and aim to serve the internet user. They refer to such matters as organising and providing universal access to information (Google), building communities and bringing the world closer together (Facebook), and empowering every person and organisation in the world (Microsoft). However, these are listed companies and profitability is a major, if not the primary goal for the shareholders. The business model adopted by tech firms is generally dependent on the number of clicks and likes, on large-scale data collection and processing, and on the provision of personalised advertising, information and services. This business model is geared towards generating content that steadily increases in appeal and sensationalism. In contrast to traditional news media, fact-finding and reliability are not guiding principles in this context. Moreover, it seems to result in an online context that is subject to different values and standards than the physical, offline world. As a result, the commercialisation of the internet feeds into dissemination of harmful online content.

Technological map of the world

According to the 2020 figures

United States

Apple	$ 1,4	trillion
Microsoft	$ 1,3	trillion
Amazon	$ 1,0	trillion
Alphabet	$ 988,7	billion
Facebook	$ 575,5	billion
Salesforce	$ 161,7	billion
Netflix	$ 151,4	billion
PayPal	$ 133,6	billion
Uber	$ 61,9	billion
Airbnb	$ 35,0	billion
Twitter	$ 25,2	billion

Asia

Alibaba	$ 554,2	billion
Tencent	$ 458,8	billion
Samsung	$ 281,2	billion
Meituan	$ 74,4	billion
JD.com	$ 55,05	billion
Baidu	$ 42,8	billion
Pinduoduo	$ 40,9	billion

Europe

SAP SE	$ 160,1	billion
Spotify	$ 26,0	billion

Africa

Naspers	$ 73,1	billion

The Netherlands

BBP	$ 913,7	billion

Figure 4: Technological map of the world. Based on The Economist (2020).

▸ 4.2 Jurisdiction over the internet

summary

The sovereignty of national governments is by definition bounded by national borders, while the internet is distinctly cross-border in nature. In the early days of the internet, its open, free nature was widely acclaimed. The emphasis was on the 'free space' and the state had no role to play there. Since then, it has become clear that some form of jurisdiction on the internet is becoming relevant from a perspective of protecting human rights.[76] This puts the concepts of territoriality and jurisdiction in a different light and they therefore deserve a renewed focus.

Given the cross-border nature of the internet, in choosing regulatory options it is vital to have knowledge of and technical expertise on the internet as a global, cross-border network of networks without central governance. The same applies to knowledge of the possible consequences of certain technological interventions. A temporary, complete shutdown of the internet, to which some governments sometimes resort, may for example make it possible to block online content to a far-reaching extent, but it also instantly paralyses all of society.

It has been established in this advisory report that the internet may well be a global public good, but it is largely in the hands of private parties. The private sector therefore has a dominant position on the internet. This means that commercial tech firms can make rules that are set out in long, often practically unreadable terms of use that almost no one actually reads. Moreover, they can implement those rules as they see fit, as well as monitor their own compliance, both in terms of technical infrastructure and the content layer of the internet. Commercial parties have thus become legislators, law enforcers and judges all in one. In a democratic society governed by the rule of law, these three functions are deliberately separated, and with good reason.

Moreover, the major tech firms can easily operate across national borders, while national governments must resort to shared jurisdiction, bilateral and multilateral negotiations, and the functioning of international organisations in order to regulate cross-border matters. The global and open nature of the internet nurtures that cross-border position held by the tech firms. As a result, it is primarily major tech firms that are dominant in internet governance at present.

In principle, countries can use the debate on regulating online content to increase their control of the internet and of the major tech firms. However, once national regulations are applied to the internet, this leads to fragmentation and the formation of a 'splinternet'. In the context of the internet, the tension between public and private domains thus reflects a tension between national sovereignty and the global nature of the internet, unfettered by jurisdiction.

Regulating the private internet sector poses an exceptional challenge. Such regulation generally takes place after the fact, once private enterprises have spent time (often extended periods) acquiring considerable power. If the plan is to use regulation to limit that position of power or change the way those companies work, such an undertaking could best be done in a process of cooperation and coordination. This is particularly relevant when companies are operating from other countries, since the options for using legislation to effectively force compliance are more limited.

As a result, content that is illegal or considered harmful in our country may still find its way into Dutch society via servers in other countries. Moreover, foreign powers can fairly easily exert influence via the internet on our democracy under the rule of law. International organisations do not have global power to take action against such influences or to counter harmful online content.

▸ 4.3 The absence of the rule of law online

In the offline world, conduct that is harmful to human rights, national security and the values of the rule of law is addressed with the assistance of the structures on which our democratic state under the rule of law is founded. The values and standards are democratically determined, open and accessible to the public, and can be enforced in a way that is appropriate under the rule of law. In that context, it is also possible to address harmful online conduct that undeniably violates national legal rules, such as child pornography. Chapter 1 already showed that it is more difficult to take action against online content that is less clearly illegal, while still acting in accordance with the values of the rule of law. For example, questions include who determines the standards of acceptable conduct on the internet (certainly now that online content is often posted in other countries), who has the position or power to assess whether these standards have been violated, and who is in a position to enforce these standards and intervene if necessary. Moreover, the online world, by its global and overwhelmingly private nature, does not have an unambiguous set of standards, and similarly lacks all the procedural safeguards at our disposal in a democratic state under the rule of law. Mechanisms that work well for law enforcement in the offline world (such as investigative powers under the authority of the Public Prosecution Service, or the ability of the neighbourhood police officer to raise suspicions) often work less well in the online context. All this means that the government cannot rely on the traditional tools and safeguards that are at its disposal in the offline world, in its efforts to counter the negative effects of the internet on human rights and the values of democracy and the rule of law. In some sense, the rule of law is currently absent in internet regulation.

▸ 4.4 The directive nature of technology

In regulating online content, it is important to acknowledge that the technology itself can also be used as a tool to influence user behaviour. As indicated in Chapter 2, technological options and design decisions determine what online content users can post and where they can post it. Examples include the 'retweet' or 'like' features, or the algorithms that determine which information will be recommended to a particular user. These design decisions can have unexpected side effects from a perspective of human rights and the rule of law. For instance, the 'retweet' feature has made it possible for shocking and insulting content to spread rapidly all over the world, although the designer did not intend for that to happen. Former Twitter developer Chris Wetherell noted in this respect: 'We might have just handed a 4-year-old a loaded weapon'.[77]

> 'We might have just handed a 4-year-old a loaded weapon.'
>
> Former Twitter developer Chris Wetherell

Technological choices are certainly not always subject to democratic oversight, and there is rarely concern for issues such as transparency and accountability. If a decision is taken to remedy this, by exercising government influence, it will have major consequences. Although this may sometimes make it possible to protect some human rights more effectively, at the same time it also puts pressure on the free and open nature of the internet.

▸ 4.5 Algorithms as both catalysts of and solutions for illegal and harmful content?

For issues regarding the regulation of online content, it is important to note the use of algorithms by nearly all internet platforms and applications in order to, for example, reach certain target audiences with a tailored message specifically for them, based on big data. That message could be commercial in nature, but it could also be political. In this way, algorithms and big data analysis are used to personalise information and for microtargeting. This means that they can generate a targeted flow of information that can strongly influence an individual's personal opinion.

Viewed in the light of human rights and internet governance, it is worth focusing attention on this use of algorithms and big data analysis. It has led to the major tech firms therefore now knowing more about the personal lives of their users than the government knows about its citizens. Moreover, internet platforms and applications can use their algorithms to influence the nature and content of disseminated information and the way people access that information. This raises the question of the extent to which citizens can still make carefully considered choices if their behaviour is influenced by personalised messages presented to them, without them realising, while they use the internet.

For the time being, algorithm use by private enterprises is subject to limited regulation, focusing primarily on data protection. Moreover, many algorithms are trade secrets, so tech firms are not transparent about the content of the algorithms and how they work. This is understandable to a certain extent, since the algorithms are part of the business model used by internet platforms and tech firms, which invest significant amounts in the development and ongoing improvement of those algorithms. At the same time, this shows that there is a gap in human rights protections in modern internet society. Protection is still primarily focused on government actions and hardly offers any answer to the question of how the commercial activities of tech firms and platforms can be reconciled with human rights.

Tech companies also use algorithms for self-regulation of harmful online content. Although huge strides are being made in developments in this field, these types of algorithms are not yet sufficiently capable of making distinctions in identifying which information is unacceptable and should therefore be removed. Moreover, algorithms cannot comprehend the context in which the content was placed on the internet, whereas context is extremely relevant. Consequently, the automatic selection of content for removal, for instance through filtering, may be rife with errors. This can lead to the freedom to share ideas and information via the intent being wrongfully restricted.

▸ 4.6 User anonymity and responsibility

User anonymity is an important feature of the internet. Even so, users also have their own responsibilities. Anonymity ensures that users are somewhat sheltered from the consequences of their actions: they can freely post anything online. Moreover, the intervention of third parties, such as digital platforms, leads to a problem of attribution and responsibility that in turn affects the range of regulatory options for the internet and the accompanying array of legal instruments. For instance, it is difficult to determine whether the response to unlawful content can only target the user, or also the platform or web forum that facilitates the content. In this context, developments within the EU regarding the adoption of a greater duty of care for hosting parties and internet platforms are relevant. However, for the time being, internet platforms exhibit only limited acceptance of the government's mandate in determining the frameworks for and extent of that duty of care.

▸ 4.7 Inadequate national coordination

Regulating online content is a relatively new issue. As stated in the introduction to this advisory report, it is not easy to arrive at international agreements, so many countries choose to follow their own path. It also became apparent from the various consultations that the AIV held for the purposes of this advisory report that there are various schools of thought within the Dutch government regarding the regulation of online content, and that there are hardly any consultative structures for determining a national position on this topic. The various ministries generally take their own independent approaches to the topic, rarely looking beyond the boundaries of their own policy competence. This means a comprehensive, national approach is lacking. As a result of this inadequate national policy coordination, efforts to ensure an international approach also leave something to be desired.

Chapter 5

Regulating online content: caught on the horns of a dilemma

From a human rights perspective, it is difficult to arrive at appropriate regulation. Active intervention in online content may be in conflict with human rights and with values of democracy and the rule of law. But the same applies to non-regulation or a passive approach to content on the internet.

▸ 5.1 Risks and dilemmas of active regulation

In making choices regarding the governance of the internet at national, regional or international level, it is necessary to acknowledge the difficult dilemmas and associated risks of regulating online content. For that reason, these dilemmas and risks have been outlined below.

- **Limiting freedom of expression and information**
  Regulating online content with the aim of protecting human rights inevitably leads to tension with other human rights and values of the rule of law. An insulting, offensive or threatening statement may be permissible from the perspective of freedom of expression but, at the same time, such a statement could lead to discrimination, reputational damage or infringement on human dignity, integrity or identity. Similarly, fake news cannot easily be rejected from the perspective of freedom of expression, but it could undermine the fundamental values of a democratic state under the rule of law if it results in unilaterally influencing and directing opinion. Consequently, protecting one human right by means of regulation creates the risk that another human right or a specific value of the rule of law is less well protected.

- **Undermining individual autonomy through regulation and enforcement**
  Active regulation and the enforcement that it necessitates (whether or not enforced by technology) generally entails a greater exercise of government power. That quickly leads to a negative impact on personal autonomy and on the protection of human rights. A quick glance at how the internet is regulated in countries such as China and Russia reveals a government that has a firm grasp on the conduct of its citizens and on the social debate taking place online.

- **Loss of the public core and the global nature of the internet**
  National regulation of online content that is enforced by technology may affect the public, free core of the internet. This creates the risk of a disintegrating and fragmented 'splinternet'. Any such 'cyber-balkanisation' would inevitably bring harm to the internet as a cross-border medium for free expression and access to information.

- **Undermining innovation and economic prosperity**
  Current regulation of online content often focuses on internet platforms and intermediaries. Making these parties liable for online content, imposing a duty of care, or limiting their freedom to do business would involve considerable risks and expenses for these parties. Business investments and the climate for new startups may become less attractive if governments decide to regulate the internet more radically.

- **Risk of counterproductive effects**
  An active, restrictive national or regional approach to regulating our own internet may legitimise efforts by foreign regimes with a dubious track record on human rights to do the same, using comparable methods, but in the pursuit of aims that are not in line with the Netherlands' human rights policy or the values of the rule of law.

summary

5.2 Risks and dilemmas of not actively regulating

A passive role on the part of governments (including the Dutch government) entails at least as many risks and dilemmas:

- **Infringing on individual rights**
  It is the task of the state to protect its citizens. If the state cannot or will not take effective action against illegal, harmful or undesirable content, the rights of those people are in jeopardy. Pertinent examples include infringements on human dignity due to discrimination and threats or insults to individuals and groups, particularly those that are vulnerable.

- **Infringing on public values and undermining the democratic state under the rule of law**
  In the event of a passive attitude towards illegal, harmful or undesirable content, public values such as social cohesion and democratic decision-making processes may be threatened. This could come about through a hardening of attitudes and polarisation of the social debate, for example, but also through deliberate disinformation campaigns, possibly launched by foreign powers with a vested interest in undermining or destabilising the democratic state under the rule of law.[78]

- **Giving foreign powers free rein**
  If the Dutch government were to adopt a conservative approach to regulating online content, both nationally and internationally, this would not prevent other states from regulating those parts of the internet that are within the scope of their influence. In China, Saudi Arabia and Iran, for instance, it has always been standard policy to block access to certain websites or temporarily shut down the entire internet (the public core of the internet). In that sense, the 'balkanisation' of the internet referenced above has already become a reality. If states were to adopt a conservative approach to regulation, it would at the same time become more difficult for them to protect their own internet and to adopt a powerful position in presenting their own values in the debate compared to those of other foreign powers.

- **Risks to security and public order**
  The internet cannot be viewed separately from the physical world. That means that online statements and actions can also have an effect in the physical world. This applies to online threats, incitement to commit criminal offences or incitement to hatred, for example, but also to the digital exchange of photos and videos of child abuse, or making preparations on the dark web for criminal or terrorist activities.[79] Non-intervention in this online world soon leads to insufficient protections for human rights and the values of the rule of law in the offline world.

- **Unfair distribution of costs and benefits**
  The business model of internet platforms is based on bringing people together and enabling them to share information with each other. When illegal, harmful or undesirable content is shared, this has a negative impact on individuals, groups and society as a whole. The costs of these negative effects are not paid by the internet platforms themselves, but by the victims and by society. It could therefore be asserted that the internet platforms create negative externalities by the act of performing their economic activities, similar to polluting industry. Professional internet platforms generally accept their social responsibility to prevent or limit these effects, but the commercial

considerations of their business models are still the deciding factor in determining the extent to which they act on their responsibility, and how. In situations involving negative externalities in which the government does not take measures to address these effects, an unfair distribution of costs and benefits between internet platforms and society may emerge.

summary

5.3 Balancing human rights in context

An open, free and secure internet is an illusion

A human rights-inclusive approach necessitates a stronger focus on the negative impact of the internet on values of democracy and the rule of law, including fundamental rights. The inherent tension between protecting human rights in specific cases, such as the possible tension between freedom of expression and the ban on discrimination, cannot and must not be disregarded.[80] Even if the guiding principle remains that the internet should be as open, free and secure as possible, it should simultaneously be beyond dispute that it is imperative to counter damage to human rights and values of democracy and the rule of law, both on and via the internet. The government can no longer avoid developing forms of regulation with a view to providing protection against harmful online content.

This is far from simple, as this advisory report clearly shows in various respects. The complications described in Chapter 4 involved in regulating online content determine and limit the options for taking action and the risks and dilemmas of regulation or non-regulation outlined above should not be disregarded. Regardless of which form(s) of regulation may be chosen, important social gains and values will often come into conflict with regulation. In addition, it will constantly be necessary to choose between different rights, including human rights, that are placed in diametric opposition by the dissemination of harmful online content. On the one hand, introducing a duty of care for internet platforms, or increasing government influence on the internet, will lead to infringement on freedom of expression, the right to access information, the right to protection of private life and freedom to conduct a business. On the other hand, non-intervention could lead to discrimination, threats to security, and the undermining of other principles of democracy and the rule of law. In searching for forms of regulation, it will therefore always be necessary to find a balance between various rights and interests – a precarious process.

A route lined with obstacles

Although many people do still use the internet unquestioningly, thanks to media, interest groups and education many users have become aware of the risks of dissemination of harmful content, disinformation and personalisation. Governments and international institutions have also become alert and active. There is political and social demand for more government regulation of online content and a more active duty of care for companies (particularly ISPs and internet platforms) when it comes to monitoring the content that end users share on the internet.[81] Moreover, that call for regulation has not only been heard in the Netherlands; traditional (Western) allies like Germany, the UK and France are also pressing for legislative measures and/or have already introduced such legislation themselves. At EU level, in a broader European context and internationally there is also an awareness of the need to take action. And action is being taken in all sorts of ways, ranging from providing recommendations for regulation and self-regulation and drafting codes of conduct to regulating specific internet applications or protecting specific fundamental rights (such as protection of personal data). Awareness of the risks posed by the internet is also reflected in various actions and reactions by major tech firms, which are investing more and more in identifying and removing harmful online content and in various forms of self-regulation.

These activities are all fairly recent, due in part to the relatively late acknowledgement of the risks and disadvantages of the internet. Moreover, it has been established above that there may be all sorts of policy initiatives and regulatory efforts, but that they take place at different levels and within various sectors – national, European, international, public and private. Effective coordination and harmonisation is lacking. The result is that the protection of fundamental rights and values of the rule of law from infringement by harmful online content is fragmented and incomplete. There are few clear international rules and provisions that can counter harmful online content. General requirements and conditions have been developed in case law in European courts like the ECtHR, but even those do not always offer equal recourse in actual practice. Moreover, a great deal of online content is not exclusively governed by EU and/or national legislation and is not subject to the jurisdiction of individual states. Neither enforcement and sanctions, nor the appropriate competences to implement such measures, have been clearly established. Self-regulation and a duty of care are in place, but they are designed rather differently across countries and sectors, or even from one company to another. This patchwork of regulatory measures also means that internet companies are faced with conflicting regulations or unclear obligations. In addition, the options for action and regulation that are customarily used at national and international level to tackle activities deemed undesirable in society (treaties, conventions, directives, binding agreements and resolutions) are not automatically aligned with internet governance and the exceptional features of the internet, as discussed extensively above – and may not be aligned at all at the core.

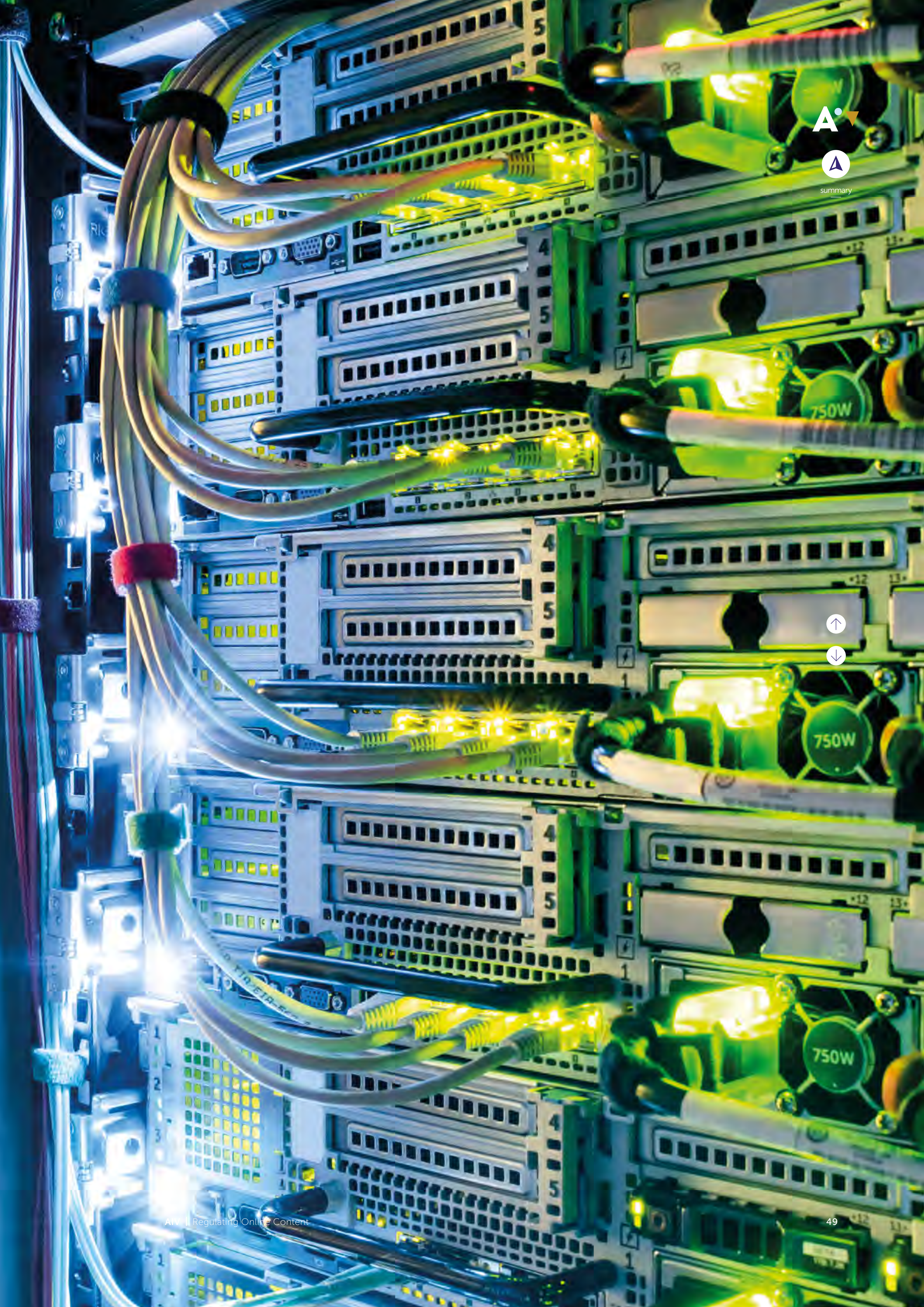
> Internet regulation cannot take place in a national cocoon. Possible courses of action to address this issue will have to be developed in an international context.

These findings illustrate that proceeding to regulate the internet not only leads to substantive dilemmas, but also raises the question of how the regulatory process can and should be designed. In that context, it is also necessary to consider the various challenges posed by the internet, as discussed in Chapter 4. The directive nature of the technology, the dominant position of private parties, the absence of the rule of law online, the fragmentary nature of the existing regulations and the lack of cross-border jurisdiction make it extremely complex to address harmful online content. These challenges in regulating the internet in general and online content in particular will be defining factors in choosing forms of regulation. To list a few examples: which private and/or public partners should be involved in the regulatory process? How fast should it happen, and in what order? And at what level of the internet should regulation be implemented?

Moreover, internet regulation cannot not take place in a national cocoon. It may be possible to impose restrictions on internet use on the basis of national legislation, but that does not prevent infringements on human rights and values of democracy and the rule of law due to harmful online content at international level, or from other countries. It therefore seems logical to seek solutions in international contexts wherever possible, even if seeking international consensus is difficult and time-consuming. The Netherlands can play a significant role at European level. The views on what constitutes harmful content are more homogeneous in Europe than at international level and there are more options for jointly establishing standards, supervision and enforcement. In addition, the Netherlands can amplify its voice more powerfully via Europe in international discussions on the regulation of online content. Human rights standards that have been laid down in relevant European conventions, such as the Lanzarote Convention and the Budapest Convention and its Additional Protocol, and the experiences from implementing them, can be used to establish similar conventions on online regulation at the level of the United Nations. The Netherlands could work with like-minded countries on initiatives to that end.

Reviewing the analysis presented in this advisory report, it must be concluded that it is necessary to recalibrate human rights policy in relation to harmful online content. At the same time, the national and international discussions regarding standards and regulation have not yet sufficiently crystallised, which has consequences for the tangible nature of the recommendations that can be made in this regard. If the Dutch government aims to achieve a human rights-inclusive approach to dealing with harmful online content, it also needs to take a number of significant strides in national internet policy. Without clear and coordinated policy at national level, regulating the internet in support of human rights at international level will become even more complex than it already is. Domestic and foreign policy should go hand in hand and align with one another. Consideration of the guiding principles set out in the summary and implementation of the recommendations in this advisory report can make a significant contribution in this regard.

summary



Endnotes

[1] The Netherlands Scientific Council for Government Policy (WRR) already noted in 'The Public Core of the Internet. An International Agenda for Internet Governance' (2015) that the internet only functions as a public good if the core values of universality, interoperability and accessibility are guaranteed and if the key objectives of information security (confidentiality, integrity and availability) are supported. In an international context, the Netherlands must also take a stand on preserving and strengthening that public core, which is shaped primarily by the core protocols and technical standards.

[2] Facebook (2019) 'Update on New Zealand'.

[3] *The Guardian* (2019) 'Social media firms fight to delete Christchurch shooting footage.'

[4] *NRC (2019)* 'Hoe het Christchurch-manifest in alle talen de wereld over gaat'.

[5] See, for example: *Washington Post* (2019) 'The internet needs new rules'; *Financial Times* (2019) 'Mark Zuckerberg: Big Tech needs more regulation' and *NRC* (2020) 'Facebook maakt werk van toezicht op moderatiebeleid'.

[6] See: Ministry of Foreign Affairs, Human Rights Report 2018.

[7] See: National Cyber Security Centre, Cyber Security Assessment Netherlands (CSBN) 2019.

[8] Parliamentary Papers 26 643, no. 447 (2016-2017).

[9] In this context, see also: AIV (2017) 'Russia and the Defence Efforts of the Netherlands', AIV advisory letter 31.

[10] See: *The Economist* (2017) 'The world's most valuable resource is no longer oil, but data'.

[11] O'Hara, Kieren en Hall, Wendy (2018) *Four Internets. The Geopolitics of Digital Governance*. CIGI Papers No. 206.

[12] See: Van Reisen, Mirjam (2018) 'Dutch National Data Policy'.

[13] See also in this context the Communication from the European Commission on a European data strategy (COM(2020) 66 final) and the White Paper on Artificial Intelligence (COM(2020) 65 final).

[14] See: Welch, Chris (2012) 'Russia, China, and other nations draft proposal to give ITU greater influence over the internet'. See also: Nye, Jr., Joseph S. (2016) 'The regime complex for managing global cyber activities', in GCIC, *Who Runs the Internet? The Global Multistakeholder Model of Internet Governance*, Chatham House, p. 8.

[15] Lynch, Colum (2019) 'China bids to lead world agency protecting intellectual property', in *Foreign Policy*.

[16] See: Negro, Gianluigi (2019) 'A history of Chinese global internet governance and its relations with ITU and ICANN', in *Chinese Journal of Communication and Financial Times* (2020) 'Inside China's controversial mission to reinvent the internet'.

[17] Lessig, L. (2006) Code v2, New York: Basic Books.

[18] This metaphor is loosely based on the work of Van Dijck, José (2019) 'Europa moet zorgen voor een diverse digitale infrastructuur', *Financieel Dagblad*; Van Dijck, José (in preparation) 'Visualizing platform power: the platformization tree'. Van Dijck's tree metaphor serves a different purpose there, however: providing specific insight into the role of large internet companies and social media platforms in our society. In this report, the main purpose of the metaphor is to depict the various parties that play a role in the world of the internet, so the tree has taken on a somewhat different shape.

[19] See: Request for Comments 1602.

[20] TCP/IP generally refers to a 'stack' of protocols. In the interests of readability, the discussion here has been limited to TCP and IP.

[21] Schermer, Bart W. and Lodder, Arno (2014) 'Internet governance' in *Recht & Computer* (6th printing), Deventer: Kluwer.

[22] Other factors that contribute to this are the good hosting and other infrastructure in the Netherlands and the presence of institutions such as SURF, which links universities of applied sciences, research universities, university hospitals, research institutions and other scientific organisations all over the world via a computer network.

[23] Until 1 October 2016, the US Department of Commerce was the supervisory authority for ICANN.

[24] See: ICANN.

[25] Resolutions are politically binding decisions that can be adopted by consensus or by vote in the Human Rights Council.

[26] See: A/HRC/RES/20/8; A/HRC/RES/26/13; A/HRC/RES/32/13 and A/HRC/RES/38/7.

[27] The International Covenant on Civil and Political Rights (ICCPR) has been ratified by 170 countries. Article 19 reads: '1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.'

[28] Ibid.

[29] Ibid.

[30] ICCPR/C/GC/34, UN Human Rights Committee, General Comment No, 34: Article 19: Freedoms of Opinion and Expression, 12 September 2011, paragraphs 12, 15 and 43.

[31] A/HRC/38/35 and A/HRC/74/486. In 2017 the Special Rapporteur also reported on the role of private actors engaged in the provision of internet and telecommunications access (A/HRC/35/22).

[32] This last provision should also be viewed in the context of the International Convention on the Elimination of all Forms of Racial Discrimination. In article 4, the States Parties to the Convention condemn 'all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination (…)'. In article 5, the States Parties to the Convention 'undertake to prohibit and to eliminate racial discrimination in all its forms and to guarantee the right of everyone, without distinction as to race, colour, or national or ethnic origin, to equality before the law (…)'.

[33] A/HRC/38/35, paragraph 1.

[34] References used for this section included: A.L.J. Janssens and A.J Nieuwenhuis (2019) *Uitingsdelicten*, 4th printing, Studiepockets Strafrecht no. 36, Wolters Kluwer, Chapter 2; J.H. Gerards, 'Artikel 10 EVRM. Vrijheid van meningsuiting', in Janneke Gerards et al. (eds.), Sdu Commentaar EVRM, The Hague: Sdu 2020; J.H. Gerards, *General Principles of the European Convention on Human Rights*, Cambridge University Press (2019); M.M. Julicher, 'Red het censuurverbod: schaf het af!', in *Tijdschrift voor Constitutioneel Recht*, July 2019, pp. 184-210.

[35] The ECtHR often (but not always) bases this on article 17 of the ECHR, which stipulates that the exercise of certain freedoms, such as freedom of expression, is not constitutionally protected if the aim is to undermine or destroy the rights and freedoms laid down in the ECHR. On this point, see e.g. P.E. de Morree, *Rights and Wrongs under the ECHR. The Prohibition of Abuse of Rights in Article 17 of the European Convention of Human Rights*, Antwerp: Intersentia, 2016.

[36] See: *Tamiz v. the United Kingdom*, ECtHR 19 September 2017, no. 3877/14; *Cengiz and Others v. Turkey*, ECtHR 1 December 2015, no. 48226/10 and 14027/11; *Ahmet Yıldırım v. Turkey*, ECtHR 18 December 2012, no. 3111/10; *Einarsson v. Iceland*, ECtHR 7 November 2017, no. 24703/15; *Kablis v. Russia*, ECtHR 30 April 2019, no. 48310/16 and 59663/17; *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, ECtHR 2 May 2016, no. 22947/13.

[37] *Delfi AS v. Estonia,* ECtHR 16 June 2015, no. 64569/09.

[38] Dutch Treaty Series 2008, 58.

[39] Dutch Treaty Series 2002, 18.

[40] Dutch Treaty Series 2003, 60.

[41] See: Council of Europe (2016) *Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg.*

[42] Recommendation No. R (97) 19.

[43] See, for example: Recommendation Rec (2001) 8; Recommendation CM/Rec (2007) 11; Recommendation CM/Rec (2008) 6; Recommendation CM/Rec (2011) 8; Recommendation CM/Rec (2014) 6; Recommendation CM/Rec (2018) 2; Declaration on freedom of communication on the internet (28 May 2003).

[44] Digital Charter (2019).

[45] The Dutch government also charts a course between the options of 'voluntary cooperation, but not without obligations, between the government and IT platforms' and binding European or national legislation. See Parliamentary Papers 30 950, no. 158 (2018).

[46] COM(2020) 65 final.

[47] COM(2020) 66 final.

[48] Directive 2000/31/EC. An EU Directive is a legally binding instrument that establishes the end result that all EU member states should achieve. The member states can then decide for themselves what national legislation must be enacted in order to reach that result.

[49] Ibid., artikel 15.

[50] Directive 2010/13/EU, article 4.

[51] Directive (EU) 2018/1808, article 1.

[52] Ibid., artikel 6.

[53] Council Framework Decision 2008/913/JHA.

[54] Directive 2011/93/EU.

[55] Directive (EU) 2017/541.

[56] See: The EU Code of Conduct (2018).

[57] See also the aforementioned Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law.

[58] European Commission (2019) *Assessment of the Code of Conduct on Hate Speech online. State of Play* (12522/19).

[59] COM(2017) 555 final.

[60] C(2018) 1177 final.

[61] COM(2018) 640 final; 2018/0331 (COD). An EU Regulation is directly applicable in all member states. Unlike a Directive, a Regulation does not have to be transposed into national law.

[62] Article 2 of the proposed Regulation defines 'terrorist content' as: 'one or more of the following information: (a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed; (b) encouraging the contribution to terrorist offences; (c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541; (d) instructing on methods or techniques for the purpose of committing terrorist offences'.

[63] Ibid., article 3.

[64] 2018/0331 (COD), consideration 5.

[65] COM(2018) 236 final.

[66] The Communication from the European Commission is based in part on the advice of the High-Level Expert Group on Fake News established by the Commission in 2017. See: European Commission (2018) Final report of the High Level Expert Group on Fake News and Online Disinformation.

[67] See: European Commission (2018) Code of Practice on Disinformation.

[68] See: European Commission (2018) Roadmaps to implement the Code of Practice on Disinformation.

[69] See: European Commission (2019) Last intermediate results of the EU Code of Practice against disinformation and European Commission (2019) Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019.

[70] JOIN(2018) 36 final.

[71] COM(2020) 65 final.

[72] See: Von der Leyen, Ursula (2019) 'A Union that strives for more. My agenda for Europe'.

[73] See: *Financial Times* (2019) 'EU draws up sweeping rules to curb illegal online content'.

[74] COM(2020) 66 final.

[75] European Commission (2019) Ethics guidelines for trustworthy AI.

[76] For a fundamental approach to these problems, see Lianne Boer and Wouter Werner, 'Concepties van territorialiteit in het internationaal recht' in *De Grenzen Voorbij. De Actualiteit van Territorialiteit en Jurisdictie*, Preadviezen Nederlandse Juristen-Vereniging 2019, Wolters Kluwer, pp. 15-58.

[77] *De Volkskrant* (2019) 'Techbedrijven moeten steeds vaker aanzien hoe hun creaties door kwaadwilligen worden gebruikt'.

[78] See also in this context AIV (2017) 'The Will of the People? The Erosion of Democracy under the Rule of Law in Europe', advisory report 104.

[79] The dark web is the part of the World Wide Web that cannot be located directly by search engines. The dark web is not used solely for illegal trade in goods and services. Journalists, human rights activists, dissidents and whistleblowers can use the dark web to exchange sensitive information anonymously.

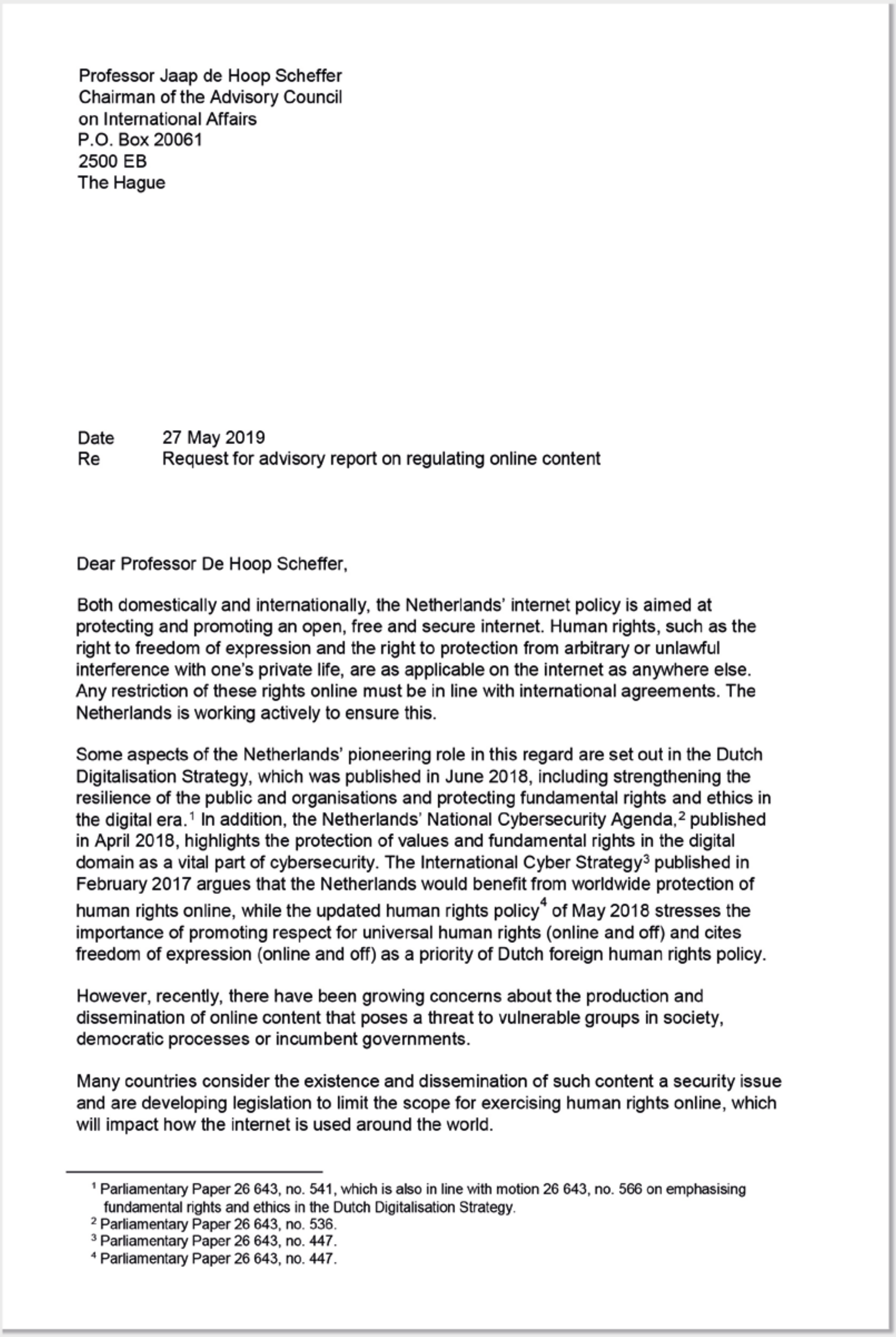
[80] This tension is constantly present in efforts to address inappropriate behaviour, for instance in criminal law (both substantive and procedural), and can never – or should never – be denied.

[81] Examples include the criminalisation of revenge porn and the desire expressed in the House of Representatives to offer better protections for privacy in horizontal relations (policy proposal on mutual privacy, submitted by MP Sven Koopmans). See: Parliamentary Papers, House of Representatives, 2017/2018, 34 926, nos. 1-2.

Annexe I

Request for advice

summary



Professor Jaap de Hoop Scheffer
Chairman of the Advisory Council
on International Affairs
P.O. Box 20061
2500 EB
The Hague

Date 27 May 2019
Re Request for advisory report on regulating online content

Dear Professor De Hoop Scheffer,

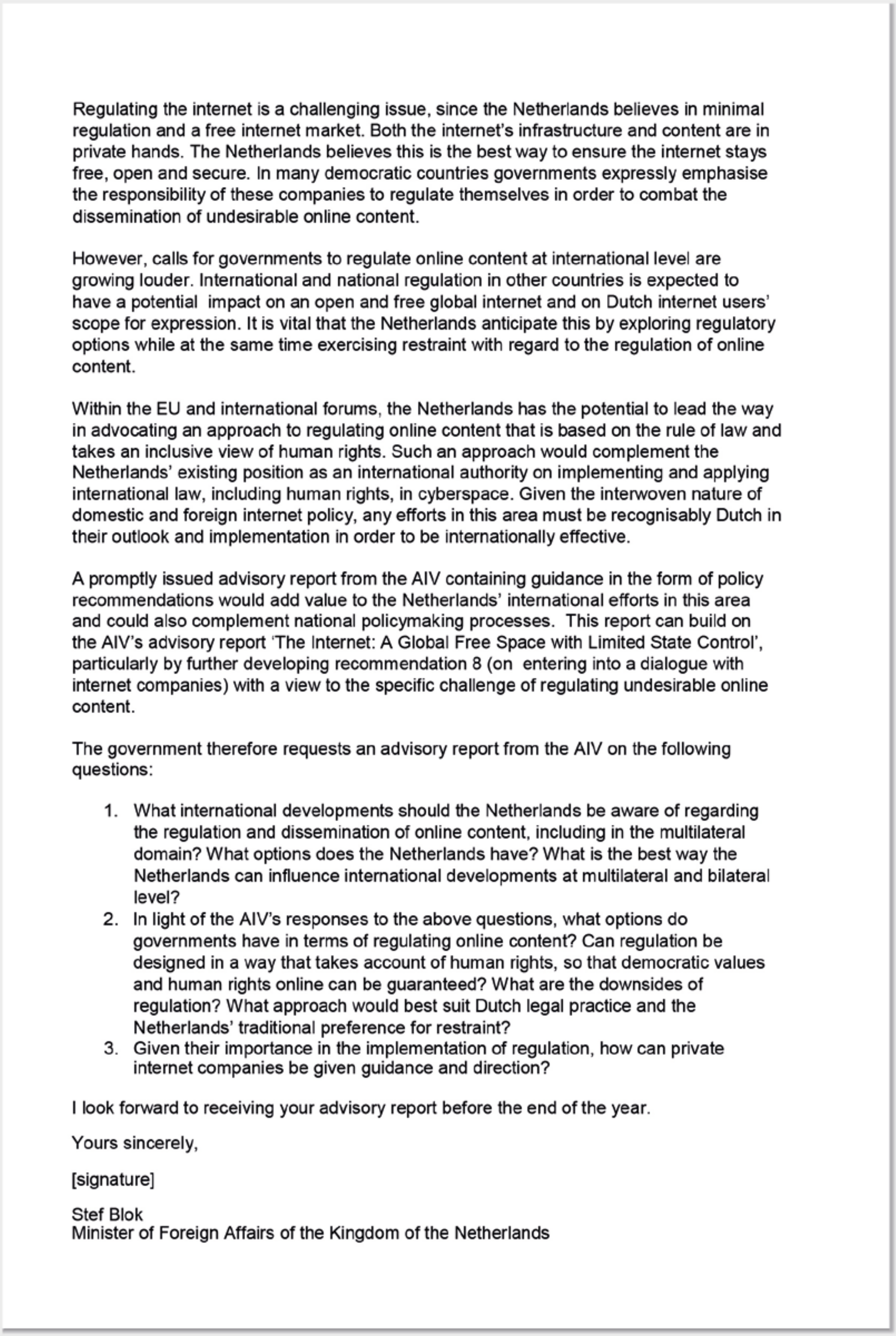
Both domestically and internationally, the Netherlands' internet policy is aimed at protecting and promoting an open, free and secure internet. Human rights, such as the right to freedom of expression and the right to protection from arbitrary or unlawful interference with one's private life, are as applicable on the internet as anywhere else. Any restriction of these rights online must be in line with international agreements. The Netherlands is working actively to ensure this.

Some aspects of the Netherlands' pioneering role in this regard are set out in the Dutch Digitalisation Strategy, which was published in June 2018, including strengthening the resilience of the public and organisations and protecting fundamental rights and ethics in the digital era.[1] In addition, the Netherlands' National Cybersecurity Agenda,[2] published in April 2018, highlights the protection of values and fundamental rights in the digital domain as a vital part of cybersecurity. The International Cyber Strategy[3] published in February 2017 argues that the Netherlands would benefit from worldwide protection of human rights online, while the updated human rights policy[4] of May 2018 stresses the importance of promoting respect for universal human rights (online and off) and cites freedom of expression (online and off) as a priority of Dutch foreign human rights policy.

However, recently, there have been growing concerns about the production and dissemination of online content that poses a threat to vulnerable groups in society, democratic processes or incumbent governments.

Many countries consider the existence and dissemination of such content a security issue and are developing legislation to limit the scope for exercising human rights online, which will impact how the internet is used around the world.

[1] Parliamentary Paper 26 643, no. 541, which is also in line with motion 26 643, no. 566 on emphasising fundamental rights and ethics in the Dutch Digitalisation Strategy.
[2] Parliamentary Paper 26 643, no. 536.
[3] Parliamentary Paper 26 643, no. 447.
[4] Parliamentary Paper 26 643, no. 447.



Regulating the internet is a challenging issue, since the Netherlands believes in minimal regulation and a free internet market. Both the internet's infrastructure and content are in private hands. The Netherlands believes this is the best way to ensure the internet stays free, open and secure. In many democratic countries governments expressly emphasise the responsibility of these companies to regulate themselves in order to combat the dissemination of undesirable online content.

However, calls for governments to regulate online content at international level are growing louder. International and national regulation in other countries is expected to have a potential impact on an open and free global internet and on Dutch internet users' scope for expression. It is vital that the Netherlands anticipate this by exploring regulatory options while at the same time exercising restraint with regard to the regulation of online content.

Within the EU and international forums, the Netherlands has the potential to lead the way in advocating an approach to regulating online content that is based on the rule of law and takes an inclusive view of human rights. Such an approach would complement the Netherlands' existing position as an international authority on implementing and applying international law, including human rights, in cyberspace. Given the interwoven nature of domestic and foreign internet policy, any efforts in this area must be recognisably Dutch in their outlook and implementation in order to be internationally effective.

A promptly issued advisory report from the AIV containing guidance in the form of policy recommendations would add value to the Netherlands' international efforts in this area and could also complement national policymaking processes. This report can build on the AIV's advisory report 'The Internet: A Global Free Space with Limited State Control', particularly by further developing recommendation 8 (on entering into a dialogue with internet companies) with a view to the specific challenge of regulating undesirable online content.

The government therefore requests an advisory report from the AIV on the following questions:

1. What international developments should the Netherlands be aware of regarding the regulation and dissemination of online content, including in the multilateral domain? What options does the Netherlands have? What is the best way the Netherlands can influence international developments at multilateral and bilateral level?
2. In light of the AIV's responses to the above questions, what options do governments have in terms of regulating online content? Can regulation be designed in a way that takes account of human rights, so that democratic values and human rights online can be guaranteed? What are the downsides of regulation? What approach would best suit Dutch legal practice and the Netherlands' traditional preference for restraint?
3. Given their importance in the implementation of regulation, how can private internet companies be given guidance and direction?

I look forward to receiving your advisory report before the end of the year.

Yours sincerely,

[signature]

Stef Blok
Minister of Foreign Affairs of the Kingdom of the Netherlands

List of persons consulted

In preparing the advisory report, the Committee spoke to many different experts. The AIV is sincerely grateful for their insights and their input.

- **Erik Akerboom**
  Commissioner of the National Police (until 29 April 2020)
- **Pieter-Jaap Aalbersberg**
  National Coordinator for Security and Counterterrorism (NCTV)
- **Arie van Bellen**
  Director of the Electronic Commerce Platform (ECP)
- **Gerrit van der Burg**
  Chair of the Board of Procurators General
- **Siobhan Cummiskey**
  Director of Public Policy, Campaigns and Programs, Facebook
- **Astrid van Engen**
  Coordinating consultant, Office of the National Coordinator for Security and Counterterrorism (NCTV)
- **Edo Haveman**
  Head of Public Policy BENELUX, Facebook
- **Arjan El Fassed**
  Head of Public Policy, Google Netherlands
- **Puck Gorrissen**
  Policy officer, Ministry of the Interior and Kingdom Relations (BZK)
- **Jochem de Groot**
  Director of Corporate Affairs, Microsoft Netherlands
- **Lauren Heida**
  Policy officer, Ministry of Defence
- **Professor Erik Huizer**
  CEO, GÉANT
- **Alex de Joode**
  Public Affairs Manager, NLdigital (until May 2020)
- **Marisa Jimenez Martin**
  Director and Deputy Head of EU Affairs, Facebook
- **Pieter van Koetsveld**
  Senior policy officer, Ministry of Education, Culture and Science (OCW)
- **Merel Koning**
  Senior policy officer, Amnesty International Netherlands
- **Ruth Kronenburg**
  Director of Operations, Free Press Unlimited
- **Lousewies van der Laan**
  Director, ICANN (until 2018)
- **Hans van Leeuwe**
  Head, Directorate-General of Policy, Ministry of Defence
- **Dr Tarlach McGonagle**
  Endowed Professor of Media Law in the Information Society, University of Leiden
- **Arienne Mulder**
  Legal specialist, Ministry of the Interior and Kingdom Relations (BZK)
- **Martinus Oosterbaan**
  Office of the National Coordinator for Security and Counterterrorism (NCTV)

- **Auke Pals**
  Chair, ECP Digiraad
- **Arnold van Rhijn**
  Senior policy officer, Ministry of Economic Affairs and Climate Policy (EZK)
- **Just Stam**
  Cabinet adviser, Ministry of Justice and Security
- **Gerard Steeghs**
  Director, Multilateral Organisations and Human Rights Department,
  Ministry of Foreign Affairs (BZ)
- **Michiel Steltman**
  Director, DINL
- **Sam Stevens**
  Public Policy Manager, Facebook
- **Marleen Stikker**
  Director, Waag Technology & Society
- **Lisa Vermeer**
  Senior policy officer, Ministry of Foreign Affairs (BZ) (until October 2019)
- **Lisa van de Voort**
  Senior policy officer for Media Policy, Ministry of Education, Culture and Science (OCW)
- **Michael Vos**
  Government Affairs Consultant, Microsoft NL
- **Maarten van Waveren**
  Senior policy officer, Ministry of Economic Affairs and Climate Policy (EZK)
- **Bastiaan Winkel**
  Policy adviser on Crime and Security, Ministry of Justice and Security
- **Guus van Zwoll**
  Senior policy officer, Ministry of Foreign Affairs (BZ)
- **Hans de Zwart**
  Director, Bits of Freedom (until October 2019)

Annexe III

List of abbreviations

summary

AIV	Advisory Council on International Affairs
GDPR	General Data Protection Regulation
EC	European Commission
ECtHR	European Court of Human Rights
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IMAP	Internet Message Access Protocol
ISP	Internet service provider
ITU	International Telecommunication Union
IP	Internet Protocol
ICCPR	International Covenant on Civil and Political Rights
EU	European Union
SMP	Social media platform
UDHR	Universal Declaration of Human Rights
UN	United Nations
US	United States
WIPO	World Intellectual Property Organization
WRR	Netherlands Scientific Council for Government Policy