ISBN 978-9934-564-52-9

TOWARDS RULE OF LAW IN THE DIGITAL ENVIRONMENT

Prepared by the
NATO Strategic Communications
Centre of Excellence

ISBN: 978-9934-564-52-9
Authors: Filippo Raso, Harvard Kennedy School of Government and Vineta Mēkone
NATO StratCom COE
Project manager: Ms. Vineta Mēkone
Line editor: Linda Curika
Copy editor: Anna Reynolds
Design: Kārlis Ulmanis

Riga, November 2019
NATO STRATCOM COE
11b Kalciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

> It is a key principle in a democratic society that those who have power must provide greater transparency.

Jānis Sārts, Director of the NATO StratCom COE

INTRODUCTION

This report summarizes an invite-only workshop held in Riga, Latvia on 12 December 2018 that focused on exploring which legal and ethical principles can promote the safety and reliability of the digital environment and reduce its risks to democracy worldwide.

The digital environment has evolved to become not only a space for rapid, cross border, and multifaceted exchange of information but also an environment that provides space for threats to human rights and national security interests. We have also learned that it has given rise to a new commodity—big data—as well as to algorithm-powered bots that mimic human behaviour. Recognising these developments, we pose the question: *Have we arrived at the point in history where we have to think about securing fundamental and human rights in the digital domain?*

In a recent publication, *Government Responses to Malicious Use of Social Media*, the NATO StratCom COE collected national legal and regulatory measures taken by 43 different governments and concluded that 'In the current, highly-politicized environment driving legal and regulatory interventions, many proposed countermeasures remain fragmentary, heavy-handed, and ill-equipped to deal with the malicious use of social media.'[1]

Although the digital industry itself has made efforts to self-regulate in order to fight disinformation in the last years, another NATO StratCom COE publication analysing the steps undertaken by Google, Twitter, and Facebook concluded that: (a) '…there is little evidence of significant changes to the companies' terms and policies, which grant extensive powers over users' content,

data, and behaviour'; (b) 'The platforms themselves have not taken any meaningful steps to get ahead of the problem and address the underlying structures that incentivize the malicious use of social media—whether for economic gain or political influence.'[2]

From the outset, workshop participants were of the same opinion that rule of law should provide a foundation for the digital environment, and that governments must do their part in achieving this while avoiding overregulation and losing the unique advantages offered by the digital domain. To strike this challenging balance, participants attempted to examine existing principles and regulations that have been used to govern similar processes in the physical domain and might be used to require greater transparency from digital actors.

The adoption of comprehensive legal and ethical principles is one possible approach that could lead to more progressive legal frameworks. Once adopted, such principles could become the foundation for national and multinational legal frameworks regarding the current digital environment and that of the future. Adopting principles based on existing fundamental and human rights will help avoid the risk of overregulating the digital environment. It will also prevent involving the international community in long theoretical discussions that would almost certainly include disagreements between democratic and authoritarian states.

Workshop organisers aimed to facilitate informed, expertise-based debates with participation from multiple stakeholders—digital actors, legal scholars, media experts, and government professionals. The day's events were organised around three central topics, described below. Experts introduced each topic to facilitate the ensuing discussion.

The first topic, **Governmental Efforts to Introduce New Legal Requirements in the Digital Environment**, examined questions such as: What are the guiding principles these efforts are based on? What are the strategic and tactical aims of the new requirements? Which government entity should oversee the new regulations and what capabilities should it have?

The experts for this topic were:

- Ms. Margit Gross, Head of the Working Group of the State Defense Law Revision Legislative Policy Department, Ministry of Justice, Republic of Estonia
- Ms. Rachael Lim Song Qi, Assistant Director (Information Policy & Plans), Ministry of Defense, Republic of Singapore

The second topic, **Extending Social, Political, and National Security Regulations to the Digital Environment**, examined questions such as: Is a digital environment free of regulations and ethical principles a vulnerability for democratic societies? Can the necessity for regulations in the digital space be compared to the necessity for regulations

in the financial sector? What is 'social media',[3] and if it is media, should current media regulations be applied? Are algorithms the new 'digital editors-in-Chief', selecting the content we consume? Should anonymous actors be allowed to advertise and advocate gatherings on 'social media', or should bots have assembly rights? How far should the Know Your Customer (KYC) requirement be applied to communication platforms?

The experts for this topic were:

- Ms. Aiga Grišāne, Head of Media Policy Division, Ministry of Culture, Republic of Latvia
- Ms. Aliona Gaidarovič, Head of the Public Information Monitoring and Expertise Unit, Office of the Journalists' Ethics, Republic of Lithuania
- Mr. Jānis Palkavnieks, Draugiem.lv, Republic of Latvia
- Prof. Daithí Mac Síthigh, Professor of Law and Innovation, Queen's University Belfast, United Kingdom
- Ms. Kadri Kaska, Research Fellow, Policy & Law, NATO Cooperative Cyber Defense Centre of Excellence, Republic of Estonia
- Mr. Giovanni De Gregorio, PhD Candidate in Public Law at University of Milano-Bicocca, Republic of Italy

The third topic, **Legal Interventions to Regulate Data Monetization and Artificial Intelligence**, examined questions such as: Are private data the new commodity? Are there existing regulations that could be adjusted to regulate private data harvesting, or should we strive to develop General Guidelines or a new network of bilateral agreements for data use on digital platforms? How should we regulate the application of AI and what principles should it be based on? Should countries establish national agencies to follow the development and application of AI in the digital environment and to what extent should the use of AI be controlled? What responsibility should websites and networks bear when their algorithms are gamed and used to spread propaganda?

The experts for this topic were:

- Ms. Kai Härmand, Deputy Secretary General of Ministry of Justice, Republic of Estonia
- Mr. Filippo Raso, Harvard Kennedy School of Government, United States

The NATO Strategic Communications Centre of Excellence hosted the event with Ms. Vineta Mēkone acting as Moderator. The appointed rapporteurs for the event were Mr. Filippo Raso (Harvard Kennedy School of Government) and Ms. Vineta Mēkone (NATO StratCom COE).

The sequence of the following chapters mirrors the order of discussions at the Workshop, complemented with an executive summary, highlights, and references.

The NATO Strategic Communications Centre of Excellence will be hosting additional discussions and further contemplation of these issues during separate workshops to be held at a later date.

> [T]echnology is an increasingly important trend in the world … [T]he question is more "what is the right regulation" rather than "should we be regulated?"[25]

Mark Zuckerberg, Co-Founder of Facebook

Chapter I: Governmental Efforts to Regulate the Digital Environment

Summary and Session Analysis

Several governments have introduced regulations seeking to improve their defences against hostile activities in the digital environment, including activities such as election meddling, hate speech, and the spread of misinformation and fake news. This panel explored the legislative approaches taken by Estonia and Singapore to address these and other concerns.

The panellists highlighted the fact that democratic societies are becoming highly digitised, with approximately half of all residents using social media.

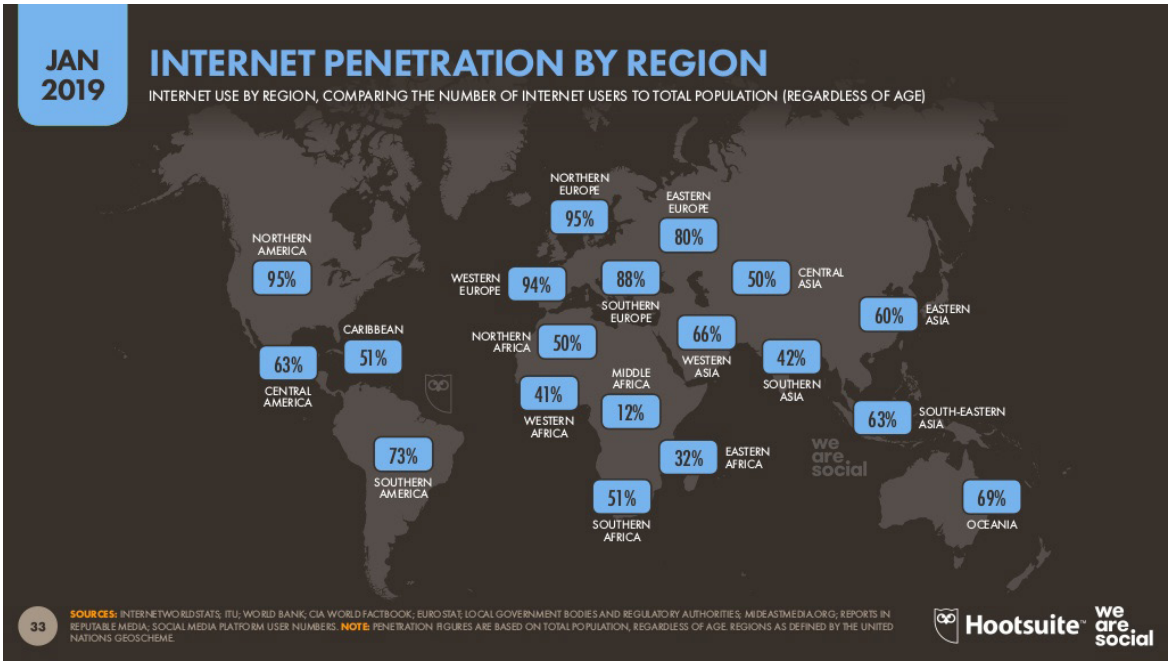


Fig. 1. Internet Penetration by Region[4]

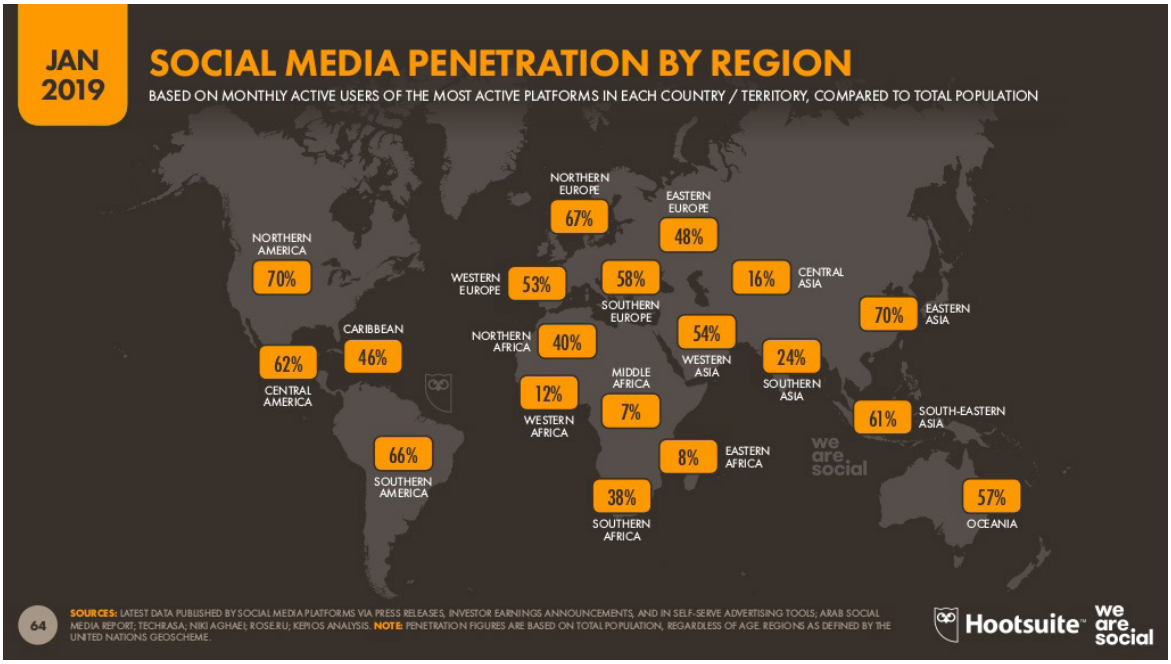


Fig. 2. Social Media Penetration by Region[5]

More people across the world are moving activities and interactions fundamental to their lives and their livelihood to the digital environment. Yet many countries lack any regulatory framework directly applicable to digital content providers and digital communications businesses. For example, 'social media' has a national legal definition in very few countries and often occupies a legal grey zone. There is no clear answer as to whether 'social media' constitute 'media' and are thus subject to existing media regulations, or whether they are something else and should be regulated separately and differently.

Yet while these abstract legal questions are being resolved, governments still need the tools to address digital threats and hostile actors, particularly as digital platforms are being abused and provide an environment in which national security can be threatened.

As a nation leading the way in digital government, Estonia has recognised that threats faced in the digital environment undermine their country's national security and cut to the core of its constitutional obligations. Estonia's national security objectives are to secure the nation's independence and sovereignty, ensure the survival of Estonian people and the state, protect the nation's territorial integrity, and maintain the country's constitutional order. The government also respects the fundamental rights and freedoms of its inhabitants while enhancing its security posture, which means the government is obliged to protect freedoms, liberties, and constitutional values when advancing its national security interests and introducing new regulations and strategies.

The Estonian government carries out strategic communications—planning and coordinating state communications and activities, as well as delivering messages to society—often through its Government Office. The government identifies and informs the public of malicious disinformation and works to decrease its influence in Estonian society by means of strategic communications. Our panellists discussed the constraints imposed on the *EU community, as, without any clear alternative or framework for dealing with the threats of the digital environment, member states are often limited in their ability to abridge individuals' freedom of expression and access to the internet. While, subject to a strict procedure, the European framework allows member states to regulate media and information society services when needed to protect public order or to safeguard national security and defence, such procedures are often time-consuming and ill-suited for rapid response.*

Under the present legal framework, the European Union and its member states have shared competence in the area of freedom, security, and justice. Yet member states have the obligation to maintain law and order and to safeguard their own internal security. With the digital environment, member states face

practical challenges in meeting their security obligations when hostile actors are abusing technologies located outside the country's borders yet operating in accordance with EU Single market rules.

The panellists discussed these threats as being an important focus for coordinated regulation for the European Union, with particular attention to the EU Single Market and the EU's shared competence to protect freedom, security, and justice. *Any such regulation should provide member states with the tools they need to protect their populations from aggressors that manipulate the media and the population by exploiting digital tools, in particular by establishing limited and well-defined circumstances when member states may impose lawful limitations on digital activities.* This would also be a prime area for international collaboration.

Despite these constraints stemming from EU law, Estonia is considering drafting an Information Society Law that would apply to all media, as well as to internet services. This comprehensive approach would replace the piecemeal legislative framework currently Estonia uses, which has separate laws for electronic devices, electronic communication services, internet services, information services, media services, and other providers.

Estonia has also adopted non-legislative means to promote a healthy digital media ecosystem: in its *Communications Handbook*, the Estonian government has committed to cooperating fully with journalists and publishers who follow the principles and values of independent journalism. The handbook expressly states that the government reserves the right to not cooperate with or accredit editorial staff belonging to media channels that are operated by foreign agents, are not independent, or do not follow proper journalistic practices. The Estonian government has also prohibited itself from promoting hostile propaganda and influence in any way.

Countries outside of the EU also regulate media to protect the values and traditions of their societies. Singapore, for example, protects its values of religious and racial harmony, stability, social cohesion, and resilience through media regulation. One of the mechanisms Singapore uses is to mandate that TV broadcasters, newspapers, and other traditional news sources be licensed by the government. After realising that digital media can also be exploited to undermine the country's values, Singapore added online news sites to the list of entities that must be licensed to operate in the country.

Starting 1 June 2013 online news sites must obtain licenses within Singapore if the site reports regularly on issues relating to Singapore and have significant reach among readers in Singapore.[6] This applies to international media outlets operating in Singapore as well. As a condition of

maintaining their licenses, TV broadcasters, newspapers, and online news sites must comply with the Singapore Internet Code of Practice that details the government's expectations of media given their ability to influence public opinion.[7] These regulations set out what the Singaporean government considers 'harmful content', which includes content that undermines racial or religious harmony.[8]

The panellists mentioned that the Government of Singapore justified applying its licensing regime to online news sites because these news providers must assume responsibility for the content they publish on their sites. The country also wanted online news providers on a more consistent regulatory framework together with traditional news platforms because Singaporeans consume media through all channels—broadcasting, print, and recently, online.

The participants discussed approaches to mitigating the threats of online media without strictly regulating online news websites. One participant proposed promoting 'fact checkers' that would verify what is being spread through the media or online. Governments would retain the power to demand that unlawful content be removed from online sites but could base their decisions on the fact checkers' determinations. The participants discussed the risks associated with such a mechanism, such as politicised or biased fact checkers, or the government ignoring fact checkers' recommendations in order to influence the media environment.

One participant raised concerns about governments having the power to regulate content because political leaders might abuse that power to promote their own political agenda. For example, political leaders might use their influence over media content to undermine the public's support of the democratic process or of the institutions that support democracy, or they might unfairly promote their own party and disparage opposition parties. *Participants discussed the need for transparency around these decisions, and for checks and balances on the power to install and implement regulations in the digital environment as, due to the nature of media and information, abuse or control of information streams becomes visible only over time.*

A robust civil society sector and a strong judicial system were described as critical components for retaining the public's trust and successfully regulating the digital environment. In many countries, civil society plays a significant role in identifying and reporting abuses of freedoms granted in the digital environment, as well as abuses by governments and private actors. For example, the Estonian Defense League has a Cyber Defense Unit, which has created the website www.propastop.org. The unit follows news on Kremlin-backed media outlets and identifies stories that contain misinformation. The unit is fully voluntary and does its work independently of the

government.

The idea was raised that not all accounts on digital and 'social media' should benefit from the same protections. Accounts operated by bots often carry as much weight (and receive as many protections) as accounts operated by real people, even though bots are used in influence campaigns. Continuing to protect these accounts jeopardizes both fundamental freedoms and governmental responsibility to promote and protect human rights. Governments must engage directly with platforms to better identify which accounts are human and which are bot operated. Failing to do so weakens individual freedoms by allowing corporate actors and foreign governments to abuse their market position and powers.

Digital platforms are more influential when disseminating opinions in contrast to public squares which were used in the past to exercise freedom of speech by members of the general public. Reach, and thus impact, via the digital environment is much greater. *To ensure that human rights and fundamental freedoms are observed in the digital environment we must insist on transparency and hold digital actors responsible.*

> We used to have more long reads, but no one is interested in this kind of stuff anymore. I decided to invest my money into something else … Something that would have more added value in business terms.[9]

Ondrej Gersl, founder of AC24.cz [10]

Chapter II: Extending the Regulation of Social, Political, and National Security Activities into the Digital Environment

Summary and Section Analysis

The second panel of the day brought together participants from private industry, academia, and government to discuss the prospect of applying existing socio-political and national security regulations to the digital environment, and to comment on potential new regulations and the objects of such regulations.

Approximately two decades ago, the global community established the key legal landscape for internet commerce by granting digital platforms, sometimes referred to as Internet Service Providers or Conduits, immunity from the actions of their users. In the United States, for example, under Section 230 of the Communications Decency Act, platforms enjoyed near-absolute immunity from the actions of their users with a few narrow exceptions. Europe adopted a similar albeit less absolute form of immunity with the e-Commerce Directive. The internet has since evolved several times, digital technologies now permeate our lives, and a few leading companies have become our primary medium for political discourse and news.

After the well-known incidents when 'social media' were used to manipulate users' political preferences and activities, national legislators have been attempting to change the legal regulations that apply to digital actors by adding requirements for social responsibility and transparency.

'Social media' are available everywhere in the world and it has been well established that digital actors are not limited by physical borders. We may still talk about language as a limitation for digital reach, but translation and other services that can breach that limitation are developing rapidly. This is leading experts to recognise that for any legal regulation applied to digital actors to be effective and helpful, it will have to be international or multilateral.

Many of the panellists supported adopting an entirely new regime for regulating 'social media' as opposed to the current approach, which focuses on incremental and gradual adjustments to existing laws. Several ideas were discussed. *The panellists considered adopting a set of legally binding principles governing the digital environment that regulators specialising in certain aspects of the online world could apply flexibly. Alternatively, a 'super regulator' could advise pre-existing regulatory bodies about the digital environment and the problems it poses.* Super regulators could be constituted as administrative bodies, independent national regulators or even international regulators, comprising a balance of representatives from industry, academia, law, civil society, and government. Yet questions remain about how such a regulator would be financed. *Panellists from the EU discussed whether member states would be able to come to a consensus about establishing an EU-wide authority, particularly in light of the varying traditions of freedom of speech and free enterprise across the Union.*

Regardless of approach, legal regulations or guidelines for digital actors should be seen as one pillar of a democratic, rule-based digital environment. The other pillars are: protecting the information infrastructure, strengthening national media, ensuring the information and media literacy of the public, and the strategic communications efforts of governments. Transparency and trust among all stakeholders are also a vital part of regulating the digital environment.

Legislating the Digital Environment in the EU Single Market

The EU market is very open and operates according to the EU Single market regulations which foresee the free movement of goods, capital, services, and labour, and is based on the 'country of origin' principle. Accordingly, an EU member state's national regulations may not apply to an entity unless that entity is registered in the respective EU country.[11]

Additionally, the recently amended EU Audiovisual Media Services Directive (AVMSD) and current regulatory framework show the complexity of regulating anything that is not well-defined. Experience has

shown that even comparatively clear-cut cases of hate speech are hard to regulate and subsequently to enforce. Recent amendments to the AVMSD have extended its scope,[12] and now the governments of EU member countries are in the process of adjusting their national legislation accordingly. The amended directive provides guidelines for cases of hate speech, but not for disinformation as such.

To minimise harms associated with the digital environment, countries could choose to regulate one or more aspects that make the most sense to supervise given their national laws, constitutions, and traditions. Various views about the pros and cons of regulating a particular aspect (objects for regulation) have been identified.

Regulation of Content

Regulation of Business model

Regulation of Process

Regulating Content
- Disinformation
- Illegal content
- Guarding free speech

Regulating Processes
- Anonymity: humans vs bots
- Transparency
- Promotion of quality news

Regulating Business Models
- Based on income sources
- Locally accountable representation
- Data ownership

Regulating AI
- Based on human rights
- Unique nature of AI
- Algorithmic transparency

Objects for Content Regulation

Hate Speech, Disinformation, Illegal Content

It was noted that the rules established in the 1990s are increasingly coming under pressure. Public perception has been gradually shifting against immunity for digital platforms on the basis that it shields these services from accountability; policymakers are questioning how they can tackle hate speech, disinformation, and other illegal content disseminated by digital actors that claim to be neutral platforms.

The concepts of disinformation, neutrality, and freedom of speech are understood differently among the various democratic countries. For example, in the US the act of burning a flag is protected under freedom of speech laws, while in most EU countries this is not accepted as freedom of speech. Similarly, the understanding of what is unlawful speech may differ from country-to-country.

The Definition of 'Social Media'

The panel discussed blurry definitions in the digital environment at length. For example, one aspect of 'social media' platforms is that they allow users to generate content from anywhere in the world, [13] but other platforms, not typically understood as 'social media', allow similar interactions through comment functionalities, user posts, and peer-to-peer messaging. One participant asked whether services that offer these functionalities should be considered 'social media' and be subject to the full array of media regulation. Disinformation, hate speech, and illegal content can be found anywhere users have the freedom to generate content. *Lithuania presumes that 'social media' is any platform where people can share and disseminate their opinions or other information;* this definition would encompass Facebook, Twitter, and YouTube, as well as any site that supports a comments section.

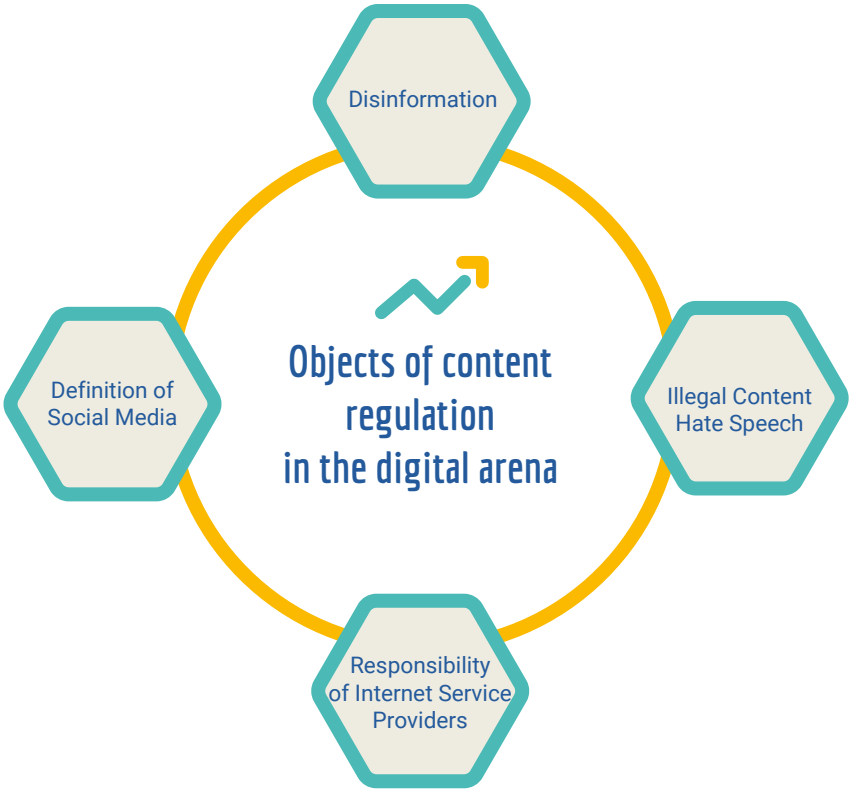
Striking a Balance Among Individuals' Rights, Free Entrepreneurship, and National Security

Several layers of complexity must be taken into account by anyone attempting to legislate online content management. In addition to provisions against censorship, the following claims must be considered:

1st layer: the constitutional right to *freedom of expression vs privacy rights, data protection, human dignity*, and the right to be informed

2nd layer: the *right of digital platforms to conduct business and provide services vs new monitoring obligations* or other new functions required by the state

3rd layer: *a country's responsibility for its own security* and the right of its population to a secure environment vs the fundamental rights and freedoms of individuals and businesses



Content moderation also has implications for the fundamental rights of users. Many people exercise their right to expression and the right to be informed through the internet. They read news, share thoughts and feelings with others, and engage in political discourse online. Although states have a constitutional duty to guarantee free speech, digital platforms have acknowledged their role as the guardians of expression in the 21st century.

In addition to the practical challenges in moderating content, platforms must address the philosophical question of whether they ought to be making speech decisions in the first place. The point was raised that 'social media' companies are private entities and, as such, often have the ability to restrict users' speech to a greater degree than do governments facing constitutional constraints.[14] *Governments may be unnecessarily burdening the rights to expression and free speech by delegating the responsibility to regulate speech to private entities.* Private entities may overpolice content by removing legitimate and lawful speech to minimize the risks of governmental fines or penalties. At the same time, private entities may underpolice content that is clearly unlawful according to local regulations by declining to remove that content absent a court order (and sometimes even with one). As business

entities, digital actors also keep in mind that users may choose another platform if they feel offended by the activities of an aggressive account or that their freedom of speech has been unduly limited.[15] Yet 'social media' as a private business does not have an obligation to provide a floor for everyone.

One panellist highlighted the trailblazing work of the European Court of Human Rights (ECHR) in evaluating the responsibilities of service providers. The ECHR has addressed content moderation issues from the perspective of the fundamental rights and human rights. These frameworks will likely play an increasingly important role in the ongoing dialogue surrounding internet regulation moving forward and, indeed, many new government papers are using this framework expressly. *The panellists agreed that policymakers may wish to consider the careful deliberations and thoughtful approach taken by the ECHR when tackling the thorny question of preserving freedom of expression online while simultaneously removing hateful, illegal, and harmful speech.*

Several cases have been deliberated in the European Court of Justice[16] with regard to requirements for online content management and the freedom of digital platforms to conduct business. In those cases, an obligation to install a particular monitoring mechanism (injunction) was considered not compliant with the European fundamental rights. The injunction was not considered proportional to the freedom of the platform to conduct business. *From the EU perspective, when governments decide to regulate online content the impact on the business of the platform has to be taken into consideration.*

The Responsibilities of Internet Service Providers

Content moderation extends beyond the 'social media' platforms. The panellists discussed how conduits of information, sometimes referred to as 'internet service providers' or 'internet access service providers', likewise have the technological ability to extensively filter and regulate the digital space. Companies acting as conduits may be required to block content in some circumstances, such as pornography websites that fail to implement age verification procedures that satisfy UK law. Yet they frequently lack clear legal authority to terminate access to other controversial or illegal materials. The participants questioned whether giving governments or private entities the authority to block or remove information would improve the exercise of fundamental rights online.

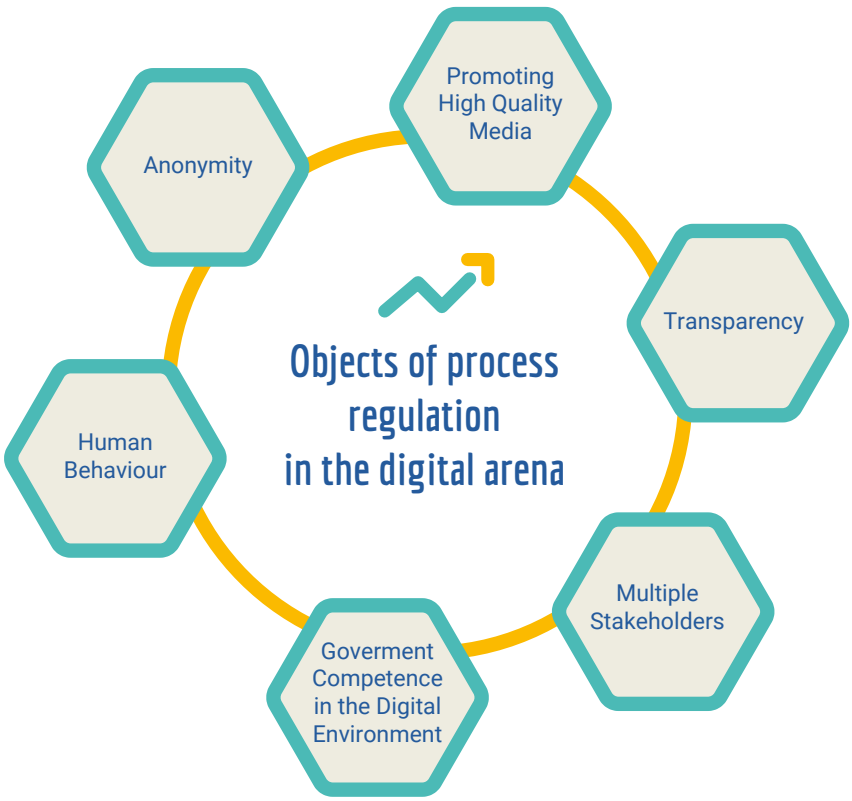
Objects for Process Regulation

Anonymity

Anonymity poses an additional hurdle to regulating illegal, harmful, and manipulative content online. User accounts can be generated simply, requiring no more than an e-mail address. 'Social media' platforms need not verify the identity of their users, allowing malicious actors to generate myriad accounts, create automated account (bot) networks, and target different segments of the population. *A full-fledged 'Know Your Customer' obligation, similar to the one imposed on financial institutions, is likely unreasonable and excessive in the digital context, but there may be wisdom is adopting a KYC-like approach for certain digital actions.*[17]

Human Behaviour

The panellists pointed out that regulations focusing on 'social media' should not lose sight of the fact that the problems encountered ultimately relate to human behaviour. While popular opinion has



grown more critical of 'social media' companies, particularly in light of the influence campaigns and individualised targeting made possible through prolific data collection and micro-targeted advertisements, the problems faced online go beyond any business model and are, ultimately, the result of human actions. *Legislators and regulators may wish to focus their efforts on problematic behaviours rather than micromanaging the business models of digital companies.*

Government Competence in the Digital Environment

Governments and high-ranking officials should recognise their responsibility to be informed about how the digital environment differs from their traditional areas of expertise. These officials should work to protect democracy and ensure that rule of law is respected online. Yet they cannot do so if they have poor knowledge and understanding of the technology and the opportunities and challenges it presents.

Unfortunately, it is common that officials identify digital issues as 'cyber' and, professing an inability to understand, disengage from these issues. Government officials need not understand the technical minutiae of every fad technology, but there should be a concerted effort to 'demystify technology', as one participant put it. The panellists agreed that officials should strive to understand enough to assess the range of human behaviour and intelligently intervene with balanced regulations that mitigate the harms we are currently experiencing. At the same time, governments must be sophisticated consumers and users of digital information. Law enforcement, for example, should follow legal processes before requesting access to users' personal data. And genuine private-sector efforts to comply with ambiguous legal standards should be recognised and supported by government.

Multiple Stakeholders in the Digital Environment

There are high expectations and demands on 'social media'; digital actors are expected not to permit crimes to be perpetrated on their platforms. Draugiem.lv raised a rhetorical question: Can the mayor of any city guarantee that no crime will be committed in their city? This comparison was made to emphasise that *preventing a crime in the digital environment is like preventing a crime in the physical domain—it must be a multilateral effort involving business, society, law enforcement, and government representatives, and all of them should be familiar with the digital issues in play*.[18]

Fundamental Rights in the Digital Environment

Countries within NATO, as well as some non-member countries, have begun developing a legal status for digital platforms, which recognises the institutional limitations

preventing 'social media' from exercising traditional editorial responsibility. Yet the proposals do require some accountability from the platforms themselves. Consider, for example, the EU's AVMSD amendments developed by the European Commission and the EU member states. The AVMSD amendments have contemplated imposing new obligations on 'video sharing services'—a type of 'social media' platform—for activities such as organising and tagging new content. *Regulations for 'social media' platforms should stem from a rights-based framework, particularly including fundamental rights. As members of all societies increasingly interact through digital means, the enjoyment of fundamental rights will grow evermore dependent on the actions of a select few private entities in the digital environment. These companies must do their part in preserving our rights.*

Simply developing new tools will not necessarily solve our problems and may create new ones. A tool intended to combat one problem may be abused to achieve entirely different aims. For example, Draugiem.lv provides users with the ability to report 'fake news' to the company for review. However, about half of all user reports are not for fake news but for materials that users found disagreeable. Other interventions may be successful in preventing virality. For example, the panellists commended Facebook's plans to limit users' abilities to share content they haven't read and WhatsApp's plan to restrict the number of times an article can be forwarded to new users. These restrictions may help shape user actions and mitigate the impact of influence operations.

The Promotion of High-quality Media

The experts discussed requiring 'social media' to promote high-quality media content. *Digital platforms could be asked to distinguish and prioritise professional media and journalism, and to convene a multi-stakeholder panel to evaluate media sources accordingly. Identifying which media outlets are of sufficient quality should be left to civil society and media experts, not to algorithms.* Media sources deemed to regularly post high-quality journalism can be given more favourable exposure. To enhance trust and transparency, the principles applied to identifying and promoting professional media should be clearly explained and accessible to all users.

Transparency

One of the key objects that regulations should address is transparency, especially: sponsored advertisements and targeted content; the application of algorithms; the platform's rules governing the collection, use, disclosure of users' personal data; and the sharing of information with researchers. *Users need greater transparency from digital service providers to ensure their rights and interests are being observed and need regulations that hold service providers responsible for enforcing users' rights.*

Regulations must be designed mindfully given constitutional constraints. Certain European courts have rejected governmental requests that private entities establish automated monitoring mechanisms on the basis of fundamental rights and the freedom of legal persons to conduct business. Rather than mandating specific actions such as automated monitoring, it may be appropriate for platforms to provide users with additional transparency and appeal mechanisms when content has been removed. These mechanisms may protect freedom of speech in the digital environment as greater regulations are imposed.

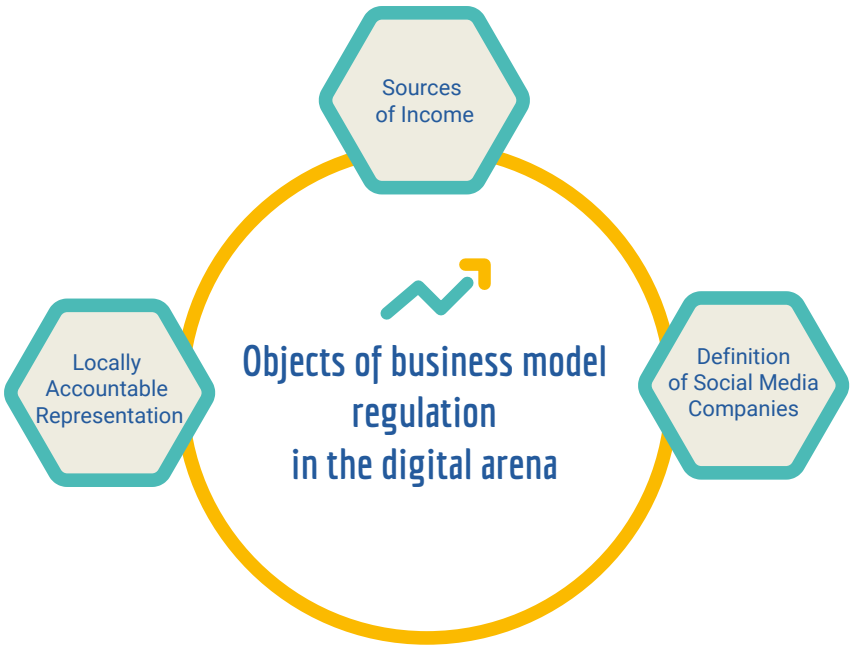
Recent high-profile scandals have involved researchers violating digital actors' Terms of Service and using personal data irresponsibly and illegally. These scandals exposed the extent to which personal data can be used to assess and manipulate peoples' behaviour and revealed that such manipulations can impact matters of national security. Additional transparency is needed to protect users, and others subsequently impacted, from these harms. *National security interests could be protected by independent national and international oversight of digital actors. States often take a more hands-on approach when national security interests could be affected by business dealings, for example financial operations and bank activities.*[19]

Objects for Business Model Regulation

The Status of 'Social Media' vis-à-vis Traditional Media

The panellists agreed that media organisations play a fundamental role in preserving, promoting, and defending both democracy and the public trust. Media organisations around the globe enjoy unique privileges and bear certain obligations to act in the public interest, yet there is no generally accepted definition of what constitutes media. And as digital media and 'social media' become increasingly prominent, existing national regulations (where such regulations exist) often fall short of addressing the issues arising in the digital environment. Professional media will remain valid in the digital era and should be strengthened by 'social media'. 'Social media' will not replace professional media.

There is no common EU regulation or definition for 'media'. Some EU member states require media companies to register and obtain a license, yet in many others media are not regulated and need not register or be licensed. There are no EU-wide regulations regarding media propaganda and disinformation.



Journalists also play an important role in the digitalised information environment and could provide guidance for governments and digital actors seeking to establish the rules that govern it. The experts participating in the workshop proposed a self-organised, international association of journalists, composed of and led by highly regarded, recognised professionals as one potential supporting body.

The panellists and participants expressly contemplated whether regulating 'social media' platforms similarly to traditional media organisations would be successful in addressing hate speech, disinformation, and other illegal activities. It was pointed out that in Singapore traditional media organisations must be licensed, and some countries have independent government watchdogs and ombudspersons that protect democracy and fundamental rights. Lithuania established The Office of the Inspector of Journalist Ethics as an independent office to protect human rights in the media. The office protects many rights, including the right of society to access unbiased, accurate, and fair information, as well as the individual's right to freedom of expression, to dignity and honour, to privacy, and to data protection; the Office also resolves conflicts between those rights. The Office makes and annual report to the public about trends and social threats in the public information domain.

Participants agreed that there are good reasons to conclude that 'social media' platforms are more akin to traditional media companies than to impartial conduits of

information and therefore should have additional responsibilities. 'Social media' platforms create a space for users to engage with one another; they allow content to be generated, shared, and spread. It is through 'social media' that content propagates online, meaning content that would otherwise never be read may be broadly consumed. Increasingly, 'social media' platforms curate content using algorithms and artificial intelligence technologies, automatically selecting what content to display. This engagement differs from the content-neutral and disengaged role of a conduit.

But traditional media regulations cannot be transposed neatly into the 'social media' context. Unlike traditional media organisations, 'social media' platforms do not control their content: users do. For example, it was noted that Draugiem.lv does not see its role as defining what the public can say, and that sentiment likely extends to other digital actors.

Additionally, traditional media regulations may include requirements that are simply ineffective online. Consider, for example, regulations that require broadcasters to carry a certain percentage of locally developed content. Simply extending traditional media regulations into the digital environment is unlikely to succeed in resolving the problems experienced online, especially since enforcing rights in the digital space can prove challenging.

Local Presence and Accountability

Content moderation is a Sisyphean task of astonishing complexity. First, the platform must identify content that might violate their community standards or applicable law.[20] In an interconnected world of users, identifying applicable law is no easy feat. Second, the company must determine whether the identified content actually violates community standards or applicable law. While automated systems may support content moderation, the bulk of this process remains driven by humans, meaning that human moderators review content to determine whether it should be removed. This is a highly contextual activity that requires appreciating cultural context.

Many 'social media' companies outsource content moderation functions to low-cost service providers including those in developing countries that may not appreciate the cultural and legal context within each jurisdiction, including local language, historical background, perceptions, stereotypes, and humour. However, with greater local knowledge and their access to users' information, 'social media' companies could improve their advance awareness about which accounts are likely to cause trouble.

'Social media' companies may prefer to have a single code of conduct for users worldwide. While having a single policy may simplify outsourcing content moderation and set, for example, an overall definition of hate speech, a code of conduct cannot determine what is

illegal according to international and national legislation. A law enforcement organisation may have difficulty enforcing national laws against 'social media' companies when the code of conduct set by the company has a lower threshold than national law and the company has no legal footprint in the country.

In this regard, what is considered a responsible presence for a digital actor, whether it be a physical presence or a designated representative, must be determined for each country or region where it has a significant number of users. Additional requirements on digital platforms should be proportionate to the reach, impact, and audiences a digital actor has in a specific country.

Different Regulations Based on Sources of Income

Legal requirements or oversight should differ depending on possible risks to national security, business systems, and society's interests associated with choices regarding a platform's income structure or major income source. For example, there are additional requirements in the banking sector for banks with a majority of clients who are non-residents versus residents.

Today, many 'social media' companies, but not all, use advertising-based business models that thrive on clicks and interaction rather than deliberate engagement. Several threats to society's interests have been discussed in this regard, including the diminishing relevance of real facts. Unless additional space is consciously created for verified information and reporting, professional journalism will continue to lose its niche on 'social media'. Another important source of income for advertising-based business models are derived from the aggregation of users' data. The European Commission has taken the first steps in legislating the use of personal data in the digital environment at the level of the EU, as have some countries on the national level. Estonian regulations clearly state that a person owns and controls their own data, regardless of which entities have received this data.

In contrast, other 'social media', such as draugiem.lv,[21] generate income in different ways: 70% of draugiem.lv's income comes from users who pay regular small monthly fees[22] and 30% comes from advertising.[23] Anybody can use draugiem.lv free of charge but access to enhanced statistics requires an additional fee. Draugiem.lv does not produce games but sells space to game producers while ensuring limits for minors. LinkedIn also recently introduced a service that generates income from users rather than from advertisers.

> The safety of civilians is at risk today. We need more urgent action, and we need it in the form of a digital Geneva Convention, rules that will protect civilians and soldiers. (...) There needs to be a new law in this space, we need regulation in the world of facial recognition in order to protect against potential abuse.'[24]
>
> Brad Smith, president of Microsoft

Chapter III: Legal Interventions to Regulate Data Monetization and Artificial Intelligence (AI)

Summary and Section Analysis

The final panel discussed what legislators should account for when drafting new legal interventions regarding artificial intelligence and innovations that enable the monetisation of personal data. The panellists called attention to the fact that laws reflect the values a society deems worth protecting and pointed to fundamental rights and international human rights as global pronouncements on values that are important. The panellists also discussed the unique traits of artificial intelligence technologies that are now complicating attempts to regulate them.

The panellists began by agreeing that the physical world and the digital world co-exist; treating them as legally separable can no longer be justified, especially as time and time again we see activities in the digital world having tangible and sometimes fatal consequences in the physical world. *'Real world' regulations are considered to apply with equal effect and force in the digital environment, even if not originally designed to respond to problems arising in the digital world. However, as many laws were passed before digital technologies became ubiquitous, or even before the internet was created, they rely on definitions that do not*

clearly apply to the digital environment, making it difficult for governments to enforce them without additional judicial interpretation. For example, an Estonian regulation had been drafted with reference to 'addresses' with the clear meaning being that of postal addresses. Yet the Estonian Supreme Court clarified that the law also applies to e-mail addresses.

The cross-border nature of the internet also complicates efforts to enforce national laws against digital actors and internet users. The entities that dominate the web commercially often lack meaningful presence in the same countries where their actions have significant impacts. In the Baltic countries, for example, Facebook has become the dominant 'social media' platform, yet the company has no established physical presence in the region. This limits the primary vehicles through which the Baltic countries can enforce their laws: fines and criminal sanctions. Other levers that might be available to governments, such as blocking access to the provider, may be limited through constitutional or regional law as discussed in Chapter II, or otherwise could be considered an attack on fundamental freedoms. As a result, many countries must rely on the good will of corporate actors or seek other possible mechanisms for enforcing their laws.

The participants proposed one alternative: acting in concert with other nations in similar positions. In response to the series of Facebook scandals, the United Kingdom's parliament conducted an inquiry into Facebook's digital media and advertising practices. Legislators from other countries joined the inquiry to amplify its profile and power to investigate.

Aside from enforcement, however, legislators must also consider the policy decisions behind existing and proposed laws. Laws enacted in response to outdated technologies may not apply neatly to the current digital environment, and may in fact have undesirable consequences, whether by allowing harmful conduct or by overregulating a space to such an extent that innovation is stifled. Consider, for example, national content requirements in most broadcasting regulations that are obsolete in the context of streaming services, as explained in Chapter II. Technological development may also reveal gaps in legislative frameworks. Simply put, it will often be the case that regulations need to change to prevent harm to and from the digital environment, and legislators should craft enforcement mechanisms carefully since many companies using these technologies are global.

It was pointed out that countries may tackle these problems differently, particularly as each country determines its own national priorities and decides how best to implement those priorities. The final form their regulations take will likely reflect each nation's historical context, culture, and legal traditions. Nations will need to

decide whether they wish to regulate digital technologies through public law or private law.

Particularly in the context of artificial intelligence, many entities hope to regulate the technology with private law through contractual relationships between organizations or with data subjects. Yet it was argued that digital technologies such as AI, and content personalisation in particular, should be regulated by public law. The power imbalance between the companies employing AI to make decisions and the data subject makes it unlikely that the terms of any interaction would be truly fair, and consumers may be unable to detect when their rights have been violated, either because the technology and underlying decisions are too complex or because the technologies are used without warning or transparency. One panellist suggested considering the creation of a product safety framework for AI, requiring all AIs to be safe for humans. Lawmakers could also mandate that data subjects 'own' their own data and have the right to direct how other entities use it, even after the data has been collected and manipulated.

Drafting legislation in the face of new technologies involves decisions that reflect national values. The panellists highlighted that regulating new technologies is simpler once questions of ethics, values, and morals have been resolved; drafting technical legislation or regulations requires clarity about the aims of the regulation. There are ongoing local and, indeed, international debates around these questions. The proposed field of 'ethical AI' is one attempt to start the dialogue around national values.

Yet it was also pointed out that we needn't reinvent the wheel. Countries, blocs, and even the international community all have adopted instruments that recognise rights reflecting the values of each community. Consider the concept of fundamental rights in the European Union. These rights are enshrined at the constitutional level and must be protected regardless of the identity of the potential infringer. The panellists agreed that it could be helpful to use the concept of fundamental rights as a basis for regulating new technologies; this approach could provide insight into the many impacts these technologies are having and allow the process to benefit from the institutions already developed to uphold fundamental rights.

A similar framework that might act as the basis of regulatory intervention could be that of international human rights. Approximately 70 years ago, the United Nations General Assembly adopted the ***Universal Declaration on Human Rights****, which established a vision of the rights to be enjoyed by all people across the globe.* In the following years, the UN drafted several treaties implementing those rights, and those treaties have been adopted by more than a hundred countries. The rights granted to individuals under the *Universal Declaration on Human Rights* have since been refined, and a robust

jurisprudence has developed showing how these rights interact and how they are applied.

And while the main signatories to international human rights have been countries, they apply directly to private entities through the UN Guiding Principles on Business and Human Rights. Specifically, under international human rights laws, businesses have a responsibility to respect human rights and to remedy violations to which they've contributed. The main mechanisms through which private entities meet these obligations is by undertaking due diligence activities such as making human rights impact assessments, engaging affected stakeholders, and monitoring negative impacts.

There was a separate discussion with respect to AI technology, which tracked closely with the points raised above with the addition of several traits specific to AI technology that should be addressed when enacting regulations. The panellists noted that AI can both improve and harm the ability of governments to apply laws equally amongst all individuals, regardless of their power and status. AI can more effectively and reliably identify suspicious activity that may reflect illegal conduct. For example, AI can be used to better detect incidents of tax fraud or falsified corporate documentation. At the same time, unscrupulous actors can use AI to escape enforcement by identifying law enforcement officers and intentionally hiding illegal conduct from their view.

Governments that seek to regulate artificial intelligence must acknowledge the unique characteristics of the technology that complicate efforts to regulate that technology. *Artificial intelligence is ushering in the 'fourth industrial revolution', meaning that much of the economic prosperity and geopolitical clout in the 21st century and beyond will stem from our ability to develop and use artificial intelligence technologies adeptly.* There are tangible improvements for individuals, too. For example, AI-powered applications can improve educational outcomes for children and have the potential to speed the spread of powerful, low-cost healthcare. Indeed, it is not hard to imagine a world where artificial intelligence improves many aspects of the human experience. Lawmakers may be wary of legislating against such technological advantages for fear of disrupting likely future benefits.

But AI programs could also be used to undermine fundamental rights. Consider, for example, image recognition software that detects emotions. Such a device could be used to evaluate the effect on individuals viewing a political leader's speech, and authoritarian governments could then target individuals based on the results.

Additionally, AI-based decisions frequently lack the transparency needed to confirm that rights are being respected. Companies may use AI without notifying their end users in a meaningful manner. And even if users are aware the technology is being used, they

often lack the technical skill to review their decisions or are prohibited from reviewing them in a meaningful way because of intellectual property laws. These issues must be addressed by future regulations and law enforcement.

Industry has been promoting the concept of an 'ethics-based framework'. 'Ethical technology' has long been the language used by engineers contemplating the impacts of their technologies. The panellists discussed some of the benefits and drawbacks to this framework. At the highest level, creating ethical technology means settling on ethical principles to govern the technology, but this concept lacks the robust international consensus that undergirds other international frameworks.

In contrast to the other frameworks described above, such as an international-human-rights or fundamental-rights-based approach, an ethics-based framework for regulating AI lacks the institutional support needed for effective enforcement. For example, the international human rights community has existing networks and communications channels but the same cannot yet be said of an international network for ethics in technology. The human rights community also has established mechanisms for interpreting the various treaty provisions whereas, at the moment, no such mechanism exists for interpreting ethical codes. The panellists acknowledged that similar institutions will develop as the concept of ethical technology matures, but they reiterated that relevant human rights institutions already exist.

Regardless of the approach favoured, the panellists were largely in agreement that a comprehensive legal framework must be created for regulating AI as technology is evolving at a pace that quickly makes narrow regulations obsolete. It was suggested that a global treaty on artificial intelligence may be warranted. The panellists agreed that the starting point for such a treaty could be the international human rights regime.

Endnotes

1 Samantha Bradshaw, Lisa-Maria Neudert, and Philip N. Howard, Government Responses to Malicious Use of Social Media, NATO Strategic Communications Centre of Excellence, Riga, November 2018, p. 12.

2 Emily Taylor, Stacie Walsh, and Samantha Bradshaw, Industry Responses to the Malicious Use of Social Media, NATO Strategic Communications Centre of Excellence, Riga, November 2018, p. 14.

3 Taking into account the topic of this report and the fact that there is no international legal definition of 'social media', the term 'social media' will be used in quotation marks throughout.

4 Simon Kemp, 'Digital 2019: Global Digital Overview', 31 January 2019. (accessed 12 September 2019)

5 Simon Kemp 'Digital 2019: Global Digital Overview', 31 January, 2019 (accessed 12 September 2019)

6 Online news sites are required to obtain an individual license from the government agency if they match all the following criteria:
- They report regularly—at least once per week for a period of over 2 months
- Discuss issues relating to Singapore—Singapore news and current affairs
- Have significant reach among readers in Singapore—visited by at least 50 000 unique IP addresses from Singapore each month for a period of over 2 months

7 Infocomm Media Development Authority of Singapore, Internet Code of Practice

8 www.gov.sg 'What is the licensing framework for online news sites all about?', 18 June 2013 (accessed 14 October 2019)

9 Filip Brokeš, 'How to Build a Disinformation Business', .coda, 26 February 2019. (accessed 12 March 2019)

10 Ondrej Gersl is the founder of AC24.cz, recognized by the Czech NGO 'European Values' as a website that publishes intentional misinformation and conspiracy theories as news.

11 Many companies, including the largest 'social media' companies, have chosen the Republic of Ireland as their 'country of origin' in the EU because of Ireland's favourable tax policy.

12 Child protection liabilities will be imposed on 'social media' with regard to their audio-visual content.

13 Draugiem.lv sees itself as media because the company provides a platform not usually available to the individual. The company provides a public platform for sharing information with an audience, and that is media. So draugiem.lv employs a small team of content managers to act upon users' reports.

14 For the draugiem.lv content managers not many cases are clear-cut. They deliberate among themselves and by live chat and rely on the experience of the company's lawyers. In some cases, they ask for advice from the Latvian State Security Service, but their guidelines are generally informal and cannot be used to legally delete a post. On another hand, draugiem.lv does not see their role as defining what a person may or may not say.

15 Draugiem.lv has attempted to fight fake news when one of Latvia's nationalistic parties in draugiem.lv asked people to bring sharp things to a protest at Riga City Council which is run by political party inclining to support Kremlin's foreign policy. Draugiem.lv deleted all those posts due to callings for bringing sharp objects to a public square. After that draugiem.lv was blamed that they are pro-Kremlin organization.

16 For example, the SABAM saga C-70/10 and C-360/10

17 Draugiem.lv knows their customers since most profiles are at least 5–10 years old and draugiem.lv can quickly identify the true intent of the user. There is a small group of troublemakers who have the potential to damage the reputation of draugiem.lv. If they are actively disruptive, a decision could be made to delete the offending account or block the IP address.

18 An example: A Draugiem.lv user reposts a YouTube link from a TV channel. The TV channel operates legally in Latvia, but the information contained in that particular video is false. What would be the legal justification for deleting the YouTube link from draugiem.lv?

19 Governmental entities overseeing financial operations have access to confidential commercial information in order to prevent money laundering, terrorism financing, and other financial crimes. These entities have rules in place to safeguard commercial secrets.

20 Public law sets what is illegal. The Terms of Service agreement created by a digital actor is a private law establishing what content will be ousted and should be in accordance with laws of a country. Terms of Service can stipulate that hate speech is not allowed, but states have different perspectives and perceptions concerning their legal regulations regarding hate speech. All democratic states share the opinion that hate speech is wrong, but the level of protection against speech in each country is different.

21 The 'social media' platform draugiem.lv was created in Latvia fourteen years ago and four years later almost every Latvian inhabitant had an account. Today draugiem.lv has around 380,000 users and 90% of the communication of

the platform takes place in Latvian. Its Terms of Service include very general and well-known points: users cannot be abusive, cannot use hate speech, etc.

22 For example, draugiem.lv charged a 50-eurocent fee per month for personal account statistics and permits users to check who is looking at their profiles and photo galleries.

23 Draugiem.lv expressly prohibits political advertisement. Politicians are allowed to have accounts but not allowed to use paid political advertisement on the platform. Other advertising on draugiem.lv follows the same rules that regulate advertising in Latvian media.

24 Robin Pagnamenta, 'Microsoft Chief Brad Smith Says Rise Of Killer Robots Is "Unstoppable"', The Telegraph, 23 September 2019. (accessed 10 October 2019)

25 David Gunton and Justin Hendrix, 'Mr Zuckerberg, Here's How You Should Be Regulated', Just Security, 23 March 2018. (accessed 14 January 2019)

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org