ROYAL NORWEGIAN MINISTRY OF
LOCAL GOVERNMENT AND MODERNISATION

Secretariat of the Human Rights Council
Advisory Committee
OHCHR - United Nations Office at Geneva
CH-1211 Geneva 10, Switzerland

Your ref	Our ref	Date
	19/4021-3	16 October 2019

Response to the Questionnaire on new and emerging digital technologies and human rights

1. Introduction

The Ministry of Local Government and Modernisation is, under the Minister of Digitalisation, responsible for the National IT-policy, for parts of the data protection policy and for policy for electronic communication. The responsibility includes, a.o., work on digitalisation and innovation in the public sector, the Personal Data Regulations and administrative responsibility for the Norwegian Data Protection Authority and the Privacy Appeals Board.

The Ministry has examined the questionnaire, and decided to answer *some of the questions* under the heading; *"Core questions"* and some of the questions under the heading; *"Questions for States."* The number of the relevant questions is marked with bold characters.

2. Core Questions

In relation to the **first question**, on how new and emerging digital technologies can help to protect and promote human rights we will highlight the following:

Universal design/ Accessibility of websites and mobile applications

New technologies can help citizens and especially people with disabilities, to get access to information online, with the use of universal design and accessibility requirements, like Web Content Accessibility Guidelines (WCAG). The principle of accessibility should be observed when designing, constructing, maintaining, and updating websites and mobile applications in order to make them more accessible to users, and in particular for persons with disabilities.

Postal address	Office address	Telephone	Department	Reference
Postboks 8112 Dep 0032 Oslo postmottak@kmd.dep.no	Akersg. 59 www.kmd.dep.no	+47 22 24 90 90 Org. nr. 972 417 858	Department of IT policy and Public Management	Anine Ung +47 22 24 68 67

This principles and guidelines for websites and mobile applications ensure access for persons with disabilities to new information and communications technologies and systems, which promotes participation in society and access to information. In this way, new technology can enable the public to receive and impart information, and thereby promote the freedom of expression in Article 10 in the Convention for the Protection of Human Rights and Fundamental Freedoms.

These principles of accessibility can also be relied upon, when designing new digital teaching tools for use in schools and academia, and thereby help students with disabilities to engage in teaching and education, and to be able to complete studies. In this way, these technologies and principles of design can promote the right to education for everyone as recognized in Article 13 of the International Covenant on Economic, Social and Cultural Rights.

Furthermore, social platforms make communication between people a lot faster, and make it easier for people arrange specific events, so people can come together for the expression and protection of their common interest in peaceful demonstrations. These technologies can therefore promote the Right to Freedom of Assembly and Association in Article 11 of the Convention of the Protection of Human Rights and Fundamental Freedoms.

Further, technologies make it also easier for people to record and document violations of human rights by public officials or others, like police-violence, and in addition, share this information with the public, using media and/or social platforms.

In relation to the **second question**, on key human rights challenges arising from new and emerging digital technologies and how these risks can be mitigated. Firstly, we do not see technology, as a threat to human rights per se, but the *use* of technologies can both protect human rights, promote human rights and constitute a threat to human rights.

Securing human rights online

As a starting point, the human rights people enjoy offline must be equally protected online. Technology can represent a way to strengthen human rights, because it allows individuals to exercise their freedom of expression due to the introduction of new forms of communication. However, increased use of technology also means that individuals are exposed to new risks, caused by the transition of human rights into the digital field. Example, the freedom of expression can be restricted due to filtering and/or blocking-technologies.

Increased surveillance: Another threat to human rights is increased surveillance, both by private companies, which gather and analyse huge amounts of data from their users, and increased surveillance of citizen's, by the governments, both secret and not secret surveillance.

The right to privacy and the protection of personal data are human rights where all restrictions must be prescribed by law and necessary in a democratic society.

The European Court of Human Rights has, in a case related to state-sponsored surveillance, in the form of bulk interception of communications, mentioned the risk such surveillance poses to democracy:

> "*In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse."* [1]

The right to respect for privacy and family life

New and emerging technologies can be seen both as a threat to privacy and as a means to protect privacy.

Technology offers new ways of protecting privacy. It is potentially easier to give data subjects access to their own data, to rectify data or to have data erased when offering digital services by providing specific log in services. Technology also enables the use of privacy by design and privacy by default, where technology itself is used to help data subjects choose services and solutions that best protect their privacy and personal data. In this way new and emerging technologies offer new ways of implementing privacy by design and good data protection practice. This, however, requires both readiness and determination to offer good data protection.

On the other hand, the use of digital technologies in many cases causes registration and processing of large amounts of personal data. In many cases this happens without the full knowledge of the data subject, as it is too complicated for most average users to understand the processing operations in digital services. This is e.g. the case when personal data is used for offering tailored online services, big data analysis or development of artificial intelligence, which may require large amounts of personal data. The more digital services we use, and the larger the leading tech companies become, the more personal data they collect and analyse. Due to very complex digital structures, it is difficult to give sufficient information to data subjects in order for them to give a fully informed consent to the use and processing of data. This threatens the data subject's ability to control processing of data concerning themselves. As information is vital to good data protection, complex digital structures processing large amounts of personal data without the full understanding of the data subjects may be seen as a threat to privacy.

The EU General Data Protection Regulation offers good data protection. However, data flows are global. Therefore, we need global data protection initiatives, principles and legislation to cater for good privacy protection regardless of where people live and what services they use.

[1] Big Brother Watch and Others v. The United Kingdom para. 308. Applications nos. 58170/13, 62322/14 and 24960/15. The case has been referred to the Grand Chamber.

In relation to question **number five**, on different approaches to help reduce any gaps in the existing system for addressing human rights challenges. We believe that a holistic and inclusive approach is a better approach to reduce any gaps in the existing system related to new challenges to human rights emerging from new digital technology, instead of focusing on a few selected technologies.

Selected technologies typically change rapidly and often replaced with new technologies. An important departure point may be to formulate laws and regulations in a technology-neutral way, so existing laws and regulations on human rights can be applied in the light of new technologies. Human rights should be safeguarded in the light of the *principals and typical characteristics* that reflect new and emerging technologies.

In modern society, technology is ever-present. Studies show that new technology is adopted faster than before. The rates of development of new technologies and their use are speeding up. The public is adopting innovations introduced more recently, more quickly.

New technologies, collection of data, cookies, profiling and more, makes it possible for businesses to personalize their products and services for its consumers. Companies all around the world have adopted this market strategy, in order to stay competitive.

With the rapid scalability of online platforms, some companies have gained significant market power due to the amount and value of data they hold. In addition, the core feature of the online platforms business model is the ability to create direct and indirect network effects at a large scale. This poses the risk of misuse of a dominant market position, restrictions on competition and preventing other companies from entering the market.[2]

3. Specific questions for States

In relation to question **number one**, on measures that have been put in place to deal with human rights risks arising from new and emerging digital technologies.

As different aspects of society gradually become digitalised, it is important to ensure that the public has equal access to information online. Norway adopted a regulation on universal design of information and communication technology (ICT) solutions in June 2013. The purpose of this regulation is to ensure universal design of information and communication technology, without causing an undue burden on government agencies and businesses.

The regulation applies to ICT solutions intended for use by the general public in Norway. The regulation covers enterprises that inform and offer their services to the public, through the use of ICT solutions. The ICT solutions covered by the regulation are network-based solutions, like websites and mobile application, and automatic devices, like ticketing machines etc.

[2] See "Data and competition policies related to platform economy," The European Council, March 29th 2019.

Digital Strategy for the Public Sector 2019 - 2025

The Ministry of Local Government and Modernisation has recently issued "Digital strategy for the public sector 2019-202015".[3] One of important action lines is increased data sharing, value creation and the "once- only" principle.

"Users should not need to provide information which the public sector has already obtained. Increased data sharing is also a prerequisite for developing seamless services across sectors and administrative levels. The public sector shall share data when it can and protect data when it must. Open public data shall be made available for reuse for developing new services and value creation in the business sector.

There is a need for enhanced competence in regulations and frameworks for data sharing and in the relationships between law and technology and between business and management models. There is also a need for more knowledge of how infrastructure in both the central and local government sectors can be adapted for data sharing. There is a need for an arena that can help data owners and users in this area and that can facilitate the exchange of experience in the public sector. Such an arena will be important in connection with developing seamless services, cross-sector digitalisation projects and work on more digitalisation-friendly regulations.[4]"

In relation to question, **number three,** on which government agency has an initiative in the decision-making of new and emerging digital technologies policies, and if the country has a special agency that exclusively deals with the issues of new and emerging digital technologies.

The Norwegian Board of Technology (NBT) advises the Norwegian Parliament and the government on opportunities and challenges of new technologies. To access their websites click here.

Government's Digitalisation Council

In order to discuss strategic cross-sectoral issues concerning digitalisation, the Prime Minister, in 2017, has set up the Government's Digitalisation Council. The council meets typically four times a year and consists of ministers with important responsibilities regarding digital policy. The increasing cross-cutting and cross-sectoral technological development, and the need to ensure coordination and progress are among the underlying motives and mandate for the Council. The Meetings are chaired by the Prime Minister. Stakeholders from industry, business organisations and academia, are invited to the meetings.

[3] Information about the Strategy can be accessed here: https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringsstrategi-for-offentlig-sektor/id2612415/. The Strategy will soon be available in English.
[4] From the Digital Strategy chapter 3.

The Council may discuss human rights issues if it is relevant to digitalisation policy.

https://www.regjeringen.no/no/aktuelt/oppretter-digitaliseringsutvalg/id2551401/

Yours sincerely

Katarina de Brisis
Deputy Director General

Anine Ung
Adviser

This document is signed electronically and has therefore no handwritten signature