GENEVA GRADUATE INSTITUTE

INTERNATIONAL AND DEVELOPMENT STUDIES

IDLO

ADVANCING THE RULE OF LAW & HUMAN RIGHTS IN DIGITAL SPACES

Human Rights and Humanitarianism

Geneva, Switzerland
December, 2022

Graduate Institute of International and Development Studies
Applied Research Project – Human Rights and Humanitarianism

Research Team:
Ikran Ali Abdirahman
Kazi Zakariya Rahman
Meike Lenzner
Samridhi Kumar

Academic Supervisor: Buğra Güngör
Teaching Assistant: Alexa-Rae Burk

Partner: International Development Law Organization
Michael James Warren
Neeraj Rana

Final Report
Word Count: 10,800 words
01 December 2022
Geneva, Switzerland

TABLE OF CONTENTS

1. Executive Summary 4
2. Background 7
3. Research Questions 8
4. Scope of Research 9
5. Existing Legal Framework 10
   - 5.1. International Legal Frameworks 10
   - 5.2. Regional Legal Frameworks 12
6. Human Rights in Digital Spaces 13
   - 6.1. Freedom of Speech and Expression 13
   - 6.2. Right to Access to Information 14
   - 6.3. Right to Privacy 15
   - 6.4. Right to Equality and Non-Discrimination 17
   - 6.5. Implications of the Foundational Research 21
7. Methodology and Research Design 22
8. Limitations 24
9. Summary of Challenges and Stakeholders 25
10. Best Practices 26
    - 10.1. States 26
    - 10.2. International Organizations 30
    - 10.3. Civil Society Organizations 31
    - 10.4. Technology Companies 35
11. Recommendations 38
12. Conclusion 41
13. Bibliography 43
14. Annexes 48

LIST OF ABBREVIATIONS

ACHPR:	African Charter on Human and Peoples' Rights
AfCFTA:	African Continental Free Trade Agreement
AI:	Artificial Intelligence
AIA:	Algorithmic Impact Assessment
APEC:	Asia-Pacific Economic Cooperation
API:	Application Programming Interface
AU:	African Union
CAHAI:	Council of Europe's *Ad Hoc* Committee on AI
CBPR:	Cross-Border Privacy Rules
CEPAL:	Economic Commission for Latin America and the Caribbean
CSO:	Civil Society Organization
DIA:	Digital, Inclusive, Accessible Support Project
EBT:	Electronic Benefit Transfer
EU:	European Union
GDC:	Global Digital Compact
GDPR:	General Data Protection Regulation
HUDERIA:	Human Rights Democracy and Rule of Law Impact Assessment
ICCPR:	International Covenant on Civil and Political Rights
ICESCR:	International Covenant on Economic, Social and Cultural Rights
IO:	International Organization
IoT:	Internet of Things
NGO:	Non-governmental organizations
OAS:	Organization of American States
OECD:	Organization of Economic Cooperation and Development
OGP:	Open Government Partnership
OHCHR:	Office of the High Commissioner of Human Rights
SCA:	Southern and Central Appalachian
STEM:	Science, Technology, Engineering and Mathematics
TANF:	Temporary Assistance for Needy Families
UDHR:	Universal Declaration of Human Rights
UNCTAD:	United Nations Conference on Trade and Development
UNESCO:	United Nations Education, Scientific and Cultural Organization

LIST OF FIGURES

Figure 1: Gender bias in Google Translate
Figure 2: Stakeholders in Digital Spaces
Figure 3: Key Challenges of Human Rights in Digital Spaces
Figure 4: Technology-related community engagement projects in SCA rural libraries
Figure 5: Ranking of technology companies' AI transparency

LIST OF TABLES

Table 1: Overview of national legislations governing digital spaces
Table 2: Ranking of technology companies' encryption level in messenger services

1. EXECUTIVE SUMMARY

OVERVIEW

The fast digitalization across the globe has infiltrated all aspects of our lives and resulted in new implications for human rights and the rule of law. These digital technologies are intertwined with societal and institutional frameworks from the use of the internet, social media, big data and algorithms to the use of artificial intelligence in public welfare schemes.

This report maps out current legal and political debates on human rights in digital spaces and gives an overview of the existing international legal framework, including hard and soft law, tailored to the specific human rights of consideration. Since the international legal landscape varies, we provide a short overview of regional legal frameworks. However, this report notes that the current legal systems are not well suited to sufficiently governing emerging technologies and have proven inadequate in the proper and effective regulation of digital spaces, ensuring the human rights of all are upheld. The review focuses on the right to privacy, freedom of expression, access to information and freedom from discrimination. These specific human rights were chosen to narrow the scope of this research and are most relevant to the digital spaces this research incorporates. The human rights of our focus are also most relevant to women and girls, marginalized, and vulnerable people.

The overarching problem statement of this report is: **What are the existing sources of people's rights in digital spaces, and how can states place human rights at the centre of law and regulation in the digital age?**

KEY CHALLENGES

As such, the new and emerging technologies have exposed shortcomings and challenges in the current international legal framework on the protection and advancement of the above stated relevant human rights in the digital space. This is demonstrated in the broad digital divide in access to and use of the digital infrastructure, services and spaces thus widening inequalities, discrimination and bias caused by algorithms and artificial intelligence, lack of adequate digital governance of digital spaces as well as limitations to the freedom of expression through censorship, disinformation, and fake news. Additionally, this report has found that there are limitations to the right to privacy in digital spaces, through data mining and exploitative commercialization of data, surveillance and monitoring.

These challenges to application and upholding of the relevant human rights have had adverse impacts on the digital inclusion of vulnerable and marginalized groups including women, girls and the poor in realizing their human rights in digital spaces.

The shortcomings have also been perpetuated by the lack of sufficient existing regulations to govern digital conduct and use of digital spaces and services by the developers, states and other users of digital technologies. There is therefore a need for new and innovative ways to apply and exercise human rights within digital spaces which will require an effective and improved regulatory framework including policies and institutional systems to be put in place to address such shortcomings. It is imperative for key stakeholders in human rights and digital spaces, including, states, international organizations, private sector including technology companies, civil society, academia, and users, to collaborate in addressing such challenges in the promotion of human rights in digital spaces and in the provision of digital services.

RECOMMENDATIONS

Taking these challenges into consideration, this report makes several recommendations to the key stakeholders in human rights and digital spaces as follows:

i) Improved digital governance

a. Development of a human rights centric internationally agreed minimum standards for digital governance by multi stakeholders

b. Establishment of a national co- regulatory approach for digital governance

ii) Narrowing the digital divide

a. Establishment of community engagement programs initiated by local authorities for bridging the digital divide

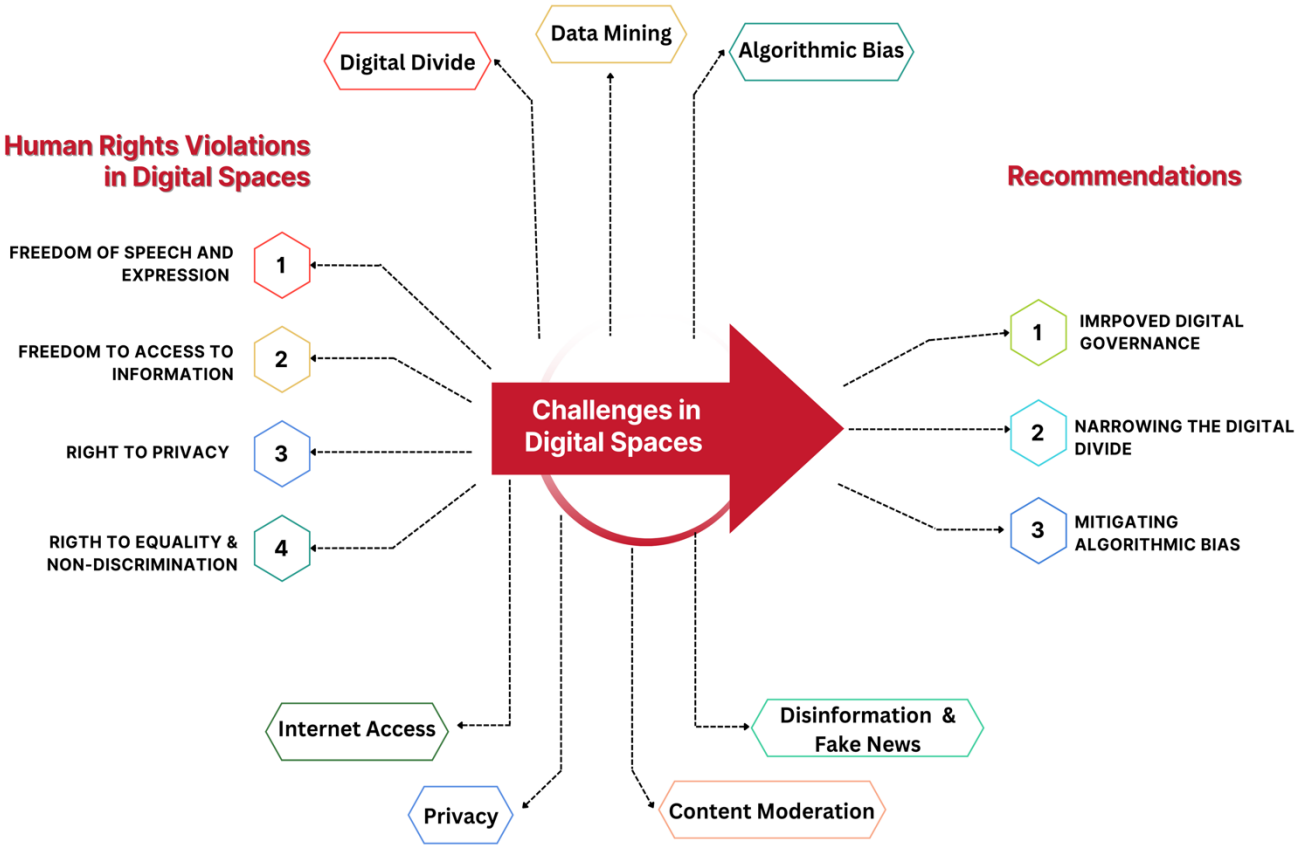
b. Collaboration of civil society and states to promote the inclusive access of governmental services

iii) Mitigating algorithmic bias

a. Technology companies, developers and users (such as governments, public and private actors) of algorithmic software should implement a bias impact assessment mechanism to probe, alert and address any potential biases and human rights violations that can result from algorithmic decisions

b. Technology companies and other developers should develop algorithmic software based on globalized data to ensure algorithmic biases are mitigated

OVERVIEW OF REPORT FINDINGS



2. BACKGROUND

Rapid advances in digital technology bring opportunities and challenges for human rights and the rule of law. Digitalization makes it easier to access public services, by moving processes online; and promoting the transparency and accountability of state institutions through the enhancement of access to information. Yet, life in the digital age also hinders the realization of human rights, including the systematic and gendered barriers to internet access ("digital divide") and challenges to privacy and free speech online. One way to mitigate these risks is to establish codified regulations that guide organizations worldwide. There is an urgent need to ensure that human rights are upheld in digital spaces through the rule of law, especially for women and girls and poor, marginalized, and vulnerable people.

IDLO, as an international organization, is specifically promoting the rule of law and justice in developing contexts. As the realm of digital spaces is opening up as a non-neglectable space for governments to protect human rights and advance the rule of law, for IDLO, this project sets the foundation to have a substantial overview of the legal and policy-related landscape of digital regulation to develop concrete projects which will further support state and private stakeholders primarily in developing countries to ensure the protection of human rights while profiting from digital developments.

This report defines digital spaces as virtual mediums, technologies, and tools individuals and entities use to connect to facilitate communication, gather information, and bolster production to fulfil their needs. Securing equal access and opportunities in the digital spaces through the promotion of human rights and the rule of law is significant for achieving the 2030 Sustainable Development Goals. Digital services are provided by diverse actors, with governments playing a central role therein. The scope of digital spaces shall be limited to social media including big data, online government services, location services, and algorithms, as these are most in line with IDLO's proposed project on Digital Innovation thematic cluster. In undertaking this research, this report will focus on four human rights relevant to digital spaces, including freedom of expression, opinion, and access to information, the right to privacy and the freedom from discrimination as more clearly described in the Annex 1.

3. RESEARCH QUESTIONS

Overarching Question:

What are the existing sources of people's rights in digital spaces, and how can states place human rights at the centre of law and regulation in the digital age?

Research Questions:

1. What are the key legal sources of people's rights in digital spaces, including multilateral agreements, national legislation, jurisprudence, and regulatory frameworks?

2. What are the key challenges facing marginalized and vulnerable groups including women, girls and the poor in realizing their rights in digital spaces?

3. Who are the key stakeholders in the global justice community relevant to the identified key challenges, including international and intergovernmental organizations, civil society networks and grassroots organizations, and private sector actors?

4. How can states place human rights at the centre of legal and regulatory frameworks on digital technologies, and uphold and extend the rule of law as technology evolves?
   - How are different relevant state actors interacting in digital legislation? What are national mechanisms and how do they live up to international standards?
   - How can the legislature ensure human rights-based legislation?
   - What role do national and international courts play in upholding the rule of law regarding technology?

5. What are the most effective legal and regulatory best practices of responding to challenges to and safeguarding human rights in digital spaces?
   - What are the best practices of international organizations and technology companies?
   - What are best practices civil society organizations have put in place to protect human rights in cases legal provisions were absent?

4. SCOPE OF RESEARCH

This report focuses on the human rights most relevant to upholding the rule of law in digital spaces, including freedom of expression, access to information, right to privacy and the freedom from discrimination. This report breaks down the international and regional legal frameworks applicable to digital spaces, focusing on hard and soft law elements. It maps the global landscape of human rights in digital spaces, identifies the legal sources and regulatory dimensions of those rights, and illuminates the key challenges and opportunities to support states in upholding people's rights in digital spaces through the rule of law.

This report focuses on these four rights as they are most relevant to this study of digital spaces and human rights. The digital space involves a high level of discourse amongst individuals, corporations and other entities. It is therefore important to ensure that there is freedom of expression guaranteed within the applicable limitation frameworks to all. Additionally, digital spaces, such as social media, utilise big data[1] and therefore, data protection and the right to privacy must be upheld (Access Now, 2018). Freedom of discrimination is directly linked to the use of social media and the provision of online government services as there is a need to ensure equal use and access to such platforms by all people including the vulnerable and marginalised individuals within society. This research focuses on these four core human rights as the specific spin off rights relevant to digital spaces and digital services are secondary to the core rights, such as, the right to be forgotten or data protection rights stem from the broad right to privacy.

The aim of this paper is to providing hands-on recommendations for IDLO in its programmatic framework, to work with its member states on how to regulate digital spaces, specifically social media, online government services, location services and algorithms, in a way to protect the most relevant digital human rights, namely freedom of speech, access to information, right to privacy and non-discrimination, ensuring the inclusion of vulnerable and marginalized people.

[1] Big data is a collection of structured, semi-structured, and unstructured data collected by organizations and used in machine learning projects, predictive modelling, and other advanced analytics applications. The more data organizations collect about users, the easier it is to "connect the dots" and understand their current behaviour, draw inferences about their future behaviour, and eventually develop deep and detailed profiles of their lives and preferences. These details are frequently extremely personal in nature, which is why even the slightest chance of them falling into the wrong hands or being misused is enough to harm user privacy.

5. EXISTING LEGAL FRAMEWORK

The existing legal framework on human rights relevant to digital spaces is a patchwork of binding and non-binding, legislations, policies and standards. This report will breakdown the current legal framework to include the varied international and regional laws and regulations below.

5.1. International Legal Frameworks

Currently, there are rights in the international legal framework that govern digital spaces, for instance, in the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), which are hard laws, meaning that they are binding legislative frameworks as opposed to soft law instruments which are non-binding. The ICCPR and ICESCR are broad and do not specifically mention digital technology, largely because both instruments predate the emergence of digital spaces. On the other hand, there are several soft law instruments that are applicable to digital spaces. For example, the United Nations (UN) Digital Road Map, the UN Interagency Dialogue on Disinformation and Data Transparency, the Human Rights Committee General Comment Number 34 and the Rabat Plan of Action. The provisions and descriptions of the rights under the hard and soft law instruments within the relevant covenants applying to digital spaces are discussed below.

Existing Universal Rights (Hard Law)

a. Freedom of expression, opinion, media, and access to information

This freedom, which encompasses the right to access information, is provided for under Article 19 of the ICCPR and Article 19 of the Universal Declaration of Human Rights (UDHR). Article 19 of the ICCPR provides that every person has the right to hold opinions without interference, and the right to freedom of expression, including the right to seek, receive and impart information through any media of choice.

b. Right to privacy

Article 17 of the ICCPR and Article 12 of the UDHR provide the right to protect privacy from arbitrary or unlawful interference. This protection also extends to the family, home, or correspondence and includes protection against unlawful attacks on one's honor and reputation. Under digital spaces, this right to privacy extends to the protection of personal data that data protection rules regulate.

c. Freedom from discrimination

Article 26 of the ICCPR and Article 7 of the UDHR highlight that all persons are equal before the law and are entitled to equal protection without discrimination. The ICESCR also mandates State Parties to ensure that economic, social, and cultural rights are exercised without discrimination based on race, color, sex, language, religion,

political or any other opinion, national or social origin, wealth, birth or any other situation. Furthermore, Article 3 of the ICESCR also makes provision for the prioritization of the equal rights of men and women to benefit from the economic, social, and cultural rights under it. This right is relevant to digital technologies, including algorithms used by the states to provide social services, ensuring equitable access to social services for all members of society.

Limitations on rights related to 'digital spaces'

Under these hard law instruments, some limitations are mentioned under the existing universal rights, which can be associated with rights relevant to digital technologies, or "digital rights." For instance, under Article 19 of the ICCPR, there is a limitation of the right of freedom of expression and opinion limited by law, for:

i. respect of the rights or reputations of others; and

ii. the protection of national security or public order (*ordre public*), or public health or morals.

As such, Article 19 puts forward a three-part test in the restriction by states of the freedom of expression, meaning the restriction must be "provided in law," "necessary," and the least intrusive method, and for public interest reasons as stated under Article 19 (3). Article 20 of the ICCPR also prohibits propaganda for war and any advocacy of national, racial, or religious hatred that leads to discrimination, hostility, or violence.

As such, these limitations have been adopted in practice to address some of the rights associated with digital rights, which include:

i. the limitation not to include hate speech, disinformation, and online harassment;

ii. the protection of the right to privacy through the data protection rules;

iii. the governance of big data to ensure proper use of such data and non-discrimination;

iv. propaganda for war; and

v. advocacy of national, racial, or religious hatred that leads to discrimination, hostility, or violence.

However, there is a need to expand the definitions of rights not governed specifically through hard law, such as the rights relevant to emerging digital spaces, which can be governed through soft law. This will provide a means to widen the definitions found under the existing hard law, making it more specific to digital rights. This will therefore address the need for clarification of human rights norms to address the infringements mentioned above to digital rights in making digital rights work for access to digital spaces and digital services. It will also assist in clarifying the use of digital technology in the service of socio-economic and cultural rights, such as the digitalization

of social security systems and accessibility for marginalized persons.

Emerging Soft Law

Several steps have been taken thus far in contributing to the field of soft law in the international framework governing digital rights. The UN has developed guidelines such as the UN Digital Road Map, which focuses on digital cooperation among stakeholders, and the UN Interagency Dialogue on Disinformation and Data Transparency which guides on digital rights in countering disinformation, and promoting data protection, and data privacy. Furthermore, the Human Rights Committee General Comment Number 34 provides further guidelines on implementing Article 19 of the ICCPR on the freedom of opinion and expression (Human Rights Committee, 2011). The Rabat Plan of Action discusses legitimate free speech and provides guidelines on identifying and responding to incitement to hatred and violence (OHCHR, 2013).

5.2. Regional Legal Frameworks

The European Union (EU), African Union, and the Americas and Pacific regions regulate digital spaces, with the former two stricter than the latter.

a. European Union

EU legislation is the most advanced, with General Data Protection Regulation (GDPR), the Digital Services Act, and the Digital Markets Act. The regulation here is especially consumer-focused. In 2022, the European Commission issued a Draft of a Declaration on Digital Rights in the EU (European Commission, 2022). All these regulations are embedded in the broader Digital Europe Programme. The various rights to freedom of expression, opinion, access to information, and privacy are also covered in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

b. African Union

The African Union established some frameworks, notably the African Continental Free Trade Agreement (AfCFTA) Protocol on e-Commerce and the African Union Convention on Cyber Security and Personal Data Protection. The African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa also covers the African region's freedom of expression and opinion (ACHPR, 2019).

c. Americas and Asia-Pacific Regions

The Americas and Asia-Pacific regions are less regulated regarding digital spaces. Mostly the regulation is only for digital markets in larger free trade agreements. For instance, the Cross-Border Privacy Rules (CBPR) developed by the Asia-Pacific Economic Cooperation (APEC) is an example of a data privacy certification supported by the government that companies adopt to show compliance with international data protection standards (APEC, 2021).

6. HUMAN RIGHTS IN DIGITAL SPACES

6.1. Freedom of speech and expression

Until very recently, the various 'big players' of digital spaces–online platforms such as Facebook, Youtube, and Twitter– disavowed governing speech online yet have always influenced online public discourses (Sander, 2020). For instance, after the riots at Capitol Hill in January 2021, technology companies took first steps in regulating speech, acknowledging that by having taken no action against conspiracy theories and disinformation on the election online, they had significantly contributed to the consolidation of public opinion (Article 19, 2021). As gatekeepers, online platforms determine which voices are allowed on their platforms and amplify voices according to their algorithms. The main policy discussion revolves around how we can better align private incentives of platform governance with the broader public interest. Content moderation, transposing international and regional law instruments have the potential to be instrumental in creating a human-rights-based approach. The goal is to put human rights at the center, which creates an inclusive environment and enables baseline predictability and stability in clear guidelines for moderation (Sander, 2020).

Systems of content moderation vary widely depending on the digital space envisioned, but online platforms generally settle into three categories: *artisanal* approaches, where small teams of human moderators do a case-by-case review of content; *community-reliant* approaches, depending on community flagging and volunteer user-moderation; and *industrial* approaches, involving algorithmic systems and bureaucracies of thousands of moderators, (Sander, 2020). Platform moderation is not static but an ongoing process that requires a plurality of actors and does not work in a vacuum. 4 sets of influences drive it:

- Corporate Philosophy
- Regulatory Compliance
- Profit Maximization
- Public Outcry

Key substantive challenges are "authentic name" requirements held by Facebook, which may marginalize members of the LGBTQ+ community and force them to deadname or expose those using pseudonyms to protect their identity (Oliva, 2020). While under-enforcement of content moderation allowing for harmful content is a challenge, *over-*enforcement of content moderation may also silence innocent groups without due process nor following the tripartite legal test of Article 19(2) of the ICCPR, thereby unjustifiably restricting their right to impart and seek information. Some case studies to consider are the over-moderation of

breastfeeding and the under-moderation of threats in Myanmar against the Rohingya (Oliva, 2020).

We may look at key process challenges, including platform transparency and oversight, as these are massive private multinational companies operating worldwide with only indirect government control. A logic of opacity governs content moderation.

6.2. Right to Access to Information

The right to access to information means promoting and protecting individuals' ability to communicate, know, and deliberate (Mathiesen, 2014). Generally, key areas of focus are disinformation, democratic principles, and the digital (gender) divide.

Accessing information in digital spaces is critical to exercising other rights, although it must be balanced against rights to control information like the right to privacy (Mathiesen, 2014). It is instrumental in realizing democratic governance principles (Neuman, 2022). Namely, transparency, accountability, and participation (Article 19, 2019).

Key actors are technological companies as they regulate many digital spaces where information may be accessed, e.g., social media or news channels (Universal Rights Group, 2021). Search engines such as Google and Bing are powerful in determining which information is more easily accessible. In addition, governments play an important role because they produce and assess huge amounts of information (UNDP, 2003).

Disinformation and fake news threaten the right to access information in digital spaces because people are not guaranteed access to the correct information (Universal Rights Group, 2021). The threshold to determine disinformation is not always clear because the protection under human rights law may also cover controversial ideas (OHCHR, 2019). Addressing disinformation requires self and co-regulation.

> ***"Effectively tackling these challenges, while respecting and protecting all human rights, including freedom of expression and access to information, requires a multi-stakeholder approach (involving governments, technology companies, and civil society), and an internationalist approach, founded on international cooperation and the sharing of good practices and lessons learnt." (Universal Rights Group, 2021)***

However, state regulation risks being stuck in the past by technology companies continuously changing their response methods (Universal Rights Group, 2021). Furthermore, government censoring and propaganda are as much a threat as disinformation (Mathiesen, 2014).

Another challenge is the digital divide. The digital divide is a broad concept that excludes people from digital spaces and services. This affects socio-economically disadvantaged, women and girls, and older people amongst others differently. For instance, poor and vulnerable people, often in

developing countries and in rural areas, lack access to digital spaces and hence to information, like in South Africa, due to costly data packages (Jacobs, 2021).

The lack of access to digital spaces like accessing Google often leads to a denial of digital services like health services or education which are basic rights. This becomes problematic for basic democratic principles because due to people's lack of access to information, they are not visible and able to influence policy priorities. They do not generate big data upon which policy decisions are made. Furthermore, many information service systems are not demand-driven towards people excluded by the digital divide. They may not be generated in their local languages, or these information systems do not understand the local structures within communities (UNDP, 2003).

As a pioneer, Ukraine has worked on making online public services accessible for people with disabilities in the framework of the Digital, Inclusive, Accessible (DIA) Support Project. UNDP Ukraine in cooperation with the Ministry of Digital Transformation in Ukraine created a digital accessibility standard, required for government websites. In 2022, the Ministry of Digital Transformation also participated for the first time at the Conference of the Parties to the Convention on the Rights of Persons with Disabilities (UNDP Ukraine, 2022).

> ***"Progress in this direction is not stopping, even during the war. All these solutions and tools will certainly reduce and eliminate digital barriers in Ukraine. UNDP strongly believes that the digitalisation of public administration should be accessible to all people in the country, including people with disabilities, so that no one is left behind, especially during the war, and Ukraine's progress is the best demonstration of this process." (UNDP Ukraine Resident Representative)***

Furthermore, the gender digital divide means multiple barriers prevent women from fully exercising their rights. For instance, lack of education in terms of awareness and digital illiteracy or social norms excluding women from an independent public life. For women's empowerment, access to information is key to gaining political and social participation and holding governments accountable (Article 19, 2019). However, international mechanisms do not follow a gender-specific approach. Likewise, national and regional legislation on information laws is gender-neutral, not acknowledging women's specific situations (Neuman, 2022).

6.3. Right to Privacy

A growing number of data-driven business models such as Facebook, Google, and Youtube capitalize on the wealth of personal data by relying on artificial intelligence tools to facilitate censorship, surveillance, and monitoring activities in digital spaces (Amnesty International, 2019). Ensuring

the right to privacy is important for tackling issues concerning data protection, pervasive surveillance, interception, hacking, data gathering, and data-driven discrimination, which can occur in digital spaces.

Additionally, the right to privacy underpins the freedom of expression, association and belief and the right to be forgotten (online). Without the right to privacy in the digital age, individuals may fail to develop their voices and formulate opinions. Furthermore, individuals may hesitate to speak their minds and fail to develop their identities. The accessibility of personal data to everyone online has raised questions regarding the right to be forgotten, which, when violated, infringes the right to privacy (Esposito, 2017). Hence, the right to privacy is a fundamental right essential for human dignity.

Violations and abuses of the right to privacy have particular implications for women, children, and vulnerable and marginalized people. Existing machine learning models can estimate a person's age, gender, occupation, and marital status from their location (Bellovin, Hutchins, and others, 2013). Bulk collection of such types of data poses serious threats to privacy and security. More alarming is that personalized data, which is often anonymized, can be de-anonymized through AI, posing a challenge to expectations of digital anonymity (Privacy International and Article 19, 2018).

Furthermore, the use of artificial intelligence for surveillance via facial recognition, sentiment algorithms, and data mining continues to raise concerns about profiling and government monitoring. In one study, machine learning was even able to identify 69% of protesters wearing caps and scarves to hide their faces (Walker, 2016). In the context of law enforcement, with the increased use of the Internet of Things (IoT) and a huge shift towards smart cities, government surveillance in countries like China and the USA with the use of CCTV cameras threatens to end anonymity and hamper other associated rights like the right to freedom of association and the fundamental right to privacy (Nolasco and Micek, 2018). Indeed, the risk of breach of data privacy involving facial recognition data has several implications such as increasing the risk of harassment, stalking and identity theft (Lively, 2021).

Cloud computing across multiple digital platforms (Mendel, Puddephatt, and others, 2012) poses another issue. Cloud computing is a new network design that saves data on remote servers rather than local desktops and laptops. Despite the positive ramifications of this technology, cloud computing creates a wide range of privacy problems. Personal data protection is threatened by the cloud computing business model, which requires users to transfer their personal data to the Internet, posing significant concerns to users' control of their data (data sovereignty). For example, cloud

computing is used by programs such as Google Docs. However, since users do not have control over their data, such data might be subject to algorithms that can reveal personal information and potentially cause security breaches.

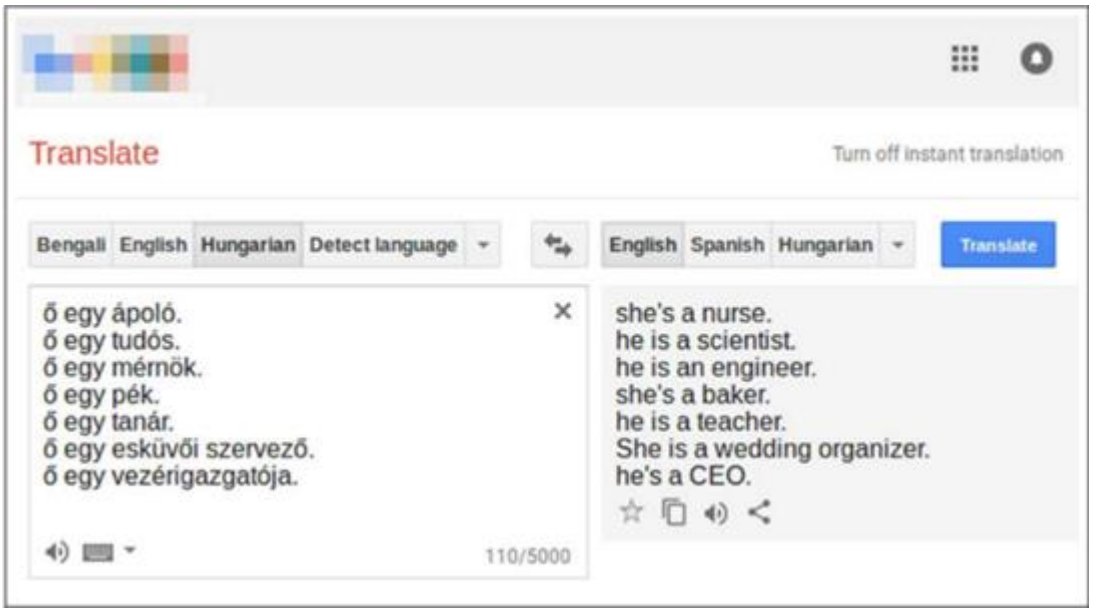
6.4. Right to Equality and Non-Discrimination

Debates in the political and scholarly realms about the right to equality and non-discrimination in digital spaces are generally concerned with thematic concerns such as digital inclusion, fair treatment, transparency, equal opportunity, access, and skills (Fjeld, Achten, and others, 2020).

As a result of a lack of good regulatory frameworks, the violation of the right to equality and non-discrimination exacerbates existing inequalities across numerous digital platforms, particularly due to the growing use of big data and AI tools. Search engines like Google have been extensively criticized for providing discriminatory results. For instance, in 2016, Google Image search results for three black teenagers gave results of three mugshots (Zuiderveen, 2020). In contrast, Google Images showed pictures of happy white kids when searching for three white kids.

Apart from racial bias, gender bias is also explicit in some search results associated with occupation. Search results have been critiqued for exaggerating gender stereotypes, portraying minorities less professionally, and even having little representation of women (Prates, Avelar, and Lamb, 2020).

Figure 1: Gender bias in Google Translate



Source: Prates, Avelar and Lamb, 2020

Prates, Avelar & Lamb (2020) did a study for the need for gender-neutral language in machine learning by providing experimental evidence that Google translate yields male defaults very frequently. This study involved utilising a comprehensive list from the U.S. Bureaur of Labor Statistics for building sentences like "He/She is an Engineer" in 12 different gender-neutral languages and then translating it into English using the Google Translate API. The results obtained exhibited a male default, particularly for fields associated with STEM jobs. For instance, Figure 1 from this study indicates that while translating sentences from gender-neutral languages like Hungarian, the result exhibited a glimpse of gender bias in machine translation. Figure 1 from Google translate indicates how occupations from traditionally male-dominated fields like CEO, engineer, and scholar are interpreted as male, while those which are traditionally female-dominated such as a nurse, baker, and wedding organiser were interpreted as female. Furthermore, another experiment in this study demonstrated that adjectives like Shy and Desirable were mostly translated with a female pronoun, whereas adjectives like Guilty and Cruel were almost entirely translated with a male pronoun. As a result, this study highlighted the need for gender-neutral language providing experimental evidence of gender bias in Google Translation results.

The right to equality and non-discrimination is further infringed by governments who rely on AI-powered software for criminal justice systems as well as for welfare schemes.

USA Criminal Justice System

For instance, the recidivism risk scoring software used across the USA criminal justice system has led to more black defendants being falsely labelled as high risk and given higher bail conditions, held in pretrial detentions and have received longer sentences (Kleinberg, J., Lakkaraju, H., Leskovec, J., Ludwig, J., & Mullainathan, S., 2018). Moreover, the facial recognition system used by law enforcement agencies raises the risk of unlawful arrests and detentions due to error and overreach. Additionally, for the last decade, AI-powered softwares has also been used for various public welfare schemes, particularly poverty management across the United States of America (Eubanks, 2018).

TANF Scandal

Policy programs like the Temporary Assistance for Needy Families (TANF) were used to determine who amongst the marginalized and the most exploited would benefit from the government schemes to automate, privatize, and reduce costs. TANF benefits were loaded on Electronic Benefit Transfer (EBT) Cards, which left a digital record whenever cash was withdrawn.

Dutch Childcare Benefit Scandal

In 2018, the Dutch childcare benefit scandal was brought to light which

exposed the discriminatory practices of the tax authorities in Netherlands (Amnesty International, 2021). The “risk categorization model”, an algorithmic decision-making mechanism, was being utilised for fraud detection. This algorithmic decision-making system used self-learning aspects such as using nationality data to develop risk profiles of childcare benefits applicants who were allegedly more inclined to submit incorrect applications and renewals, as well as potentially conduct fraud. The parameter of nationality ultimately led to non-Dutch citizens obtaining higher risk scores, amounting to racial profiling.

This scandal highlights that it is evident that such digital scrutiny and intentional use of personal data was intended to reinforce the marginality of the exploited populations and heap stigma around social programs by using automated eligibility systems and ranking algorithms. These systems are being integrated into our lives at a breath-taking pace and risk discriminating against the marginalized communities who bear a much heavy burden of being monitored, tracked, and singled out than the advantaged groups. This is not limited to the Netherlands because governments are increasingly turning to automated digital tools and algorithms to rank and rate which struggling families to support the most while making decisions on medical aid, housing, or managing poverty. It is algorithms and not humans making these calls.

RELEVANT HUMAN RIGHTS

	Freedom of expression, opinion and media	Right to privacy	Right of access to information	Freedom from discrimination
Digital divide - gender, socio-economic, age, disability inequalities	☑		☑	☑
Data mining - data as knowledge, commercialisation		☑		
Algorithmic bias - gender bias, racial bias, hiring bias, racial risk profiling				☑
Internet access - accessing digital spaces and digital services	☑		☑	☑
Privacy - surveillance, and monitoring		☑		
Content moderation - harmful content and censorship issues	☑	☑	☑	☑
Disinformation and fake news - influencing decision-making and need for verification	☑		☑	☑

6.5. Implications of the Foundational Research

The provided research has generated a good understanding of the international legal landscape to regulate digital spaces and the most pressing challenges the protection of human rights faces. Furthermore, we have achieved a better understanding of the broad spectrum of actors besides states in the regulation of digital spaces. These key challenges and actors will be portrayed graphically in the following. Through the analysis of four human rights more closely, we have been able to map out a differentiation of spaces and services, which will be crucial to proceed our research more comprehensively. While digital spaces refers to being online and being connected to platforms as such, digital services refer to interaction between actors, like individuals and governments or technology companies. Digital spaces representing connectivity and access to platforms is a necessary condition to being able to use digital services. The regulation of digital spaces therefore has a direct impact on how digital services can be used and offered.

As the above sections have provided a good foundation to go more into depth regarding the two first research questions in order to tie it specifically to the IDLO context, it has also provided a starting point to focus our research mainly on best practices of various actors and draw policy recommendations for states to safeguard the rule of law and human rights in digital spaces.

7. METHODOLOGY & RESEARCH DESIGN

This report identifies the key challenges to upholding human rights and the rule of law in digital spaces and the subsequent regulatory opportunities for states. To achieve these objectives, we intend to apply qualitative data in the research methodology with a focus on an inductive research approach by analyzing various primary and secondary sources to answer the research questions (Neuman, 2014).

These will primarily include desk-based research and analysis of primary sources such as legal instruments and internationally negotiated resolutions, and secondary sources such as policy papers, academic and grey literature including the output of key thinkers in this field. By analyzing existing legal frameworks and how they deal with challenges, we intend to observe patterns of shortcomings and develop recommendations on how states can overcome these challenges. The above-mentioned secondary sources will substantiate the preliminary research findings by reviewing the primary legal framework instruments and interviews.

Moreover, we will also collect primary data through interviews with experts at global and regional levels, including public officials, representatives of the human rights and technology sector, experts from UN agencies and international stakeholders, policymakers, civil society activists, and academic scholars among others. We intend to sample heterogeneously, picking potential interviewees from different fields to ensure diversity and inclusivity of various perspectives (Tongco, 2007). Selecting interviewees will be done in conjunction with IDLO. Such interviews will highlight emerging trends and challenges and illuminate potential opportunities and policy priorities from a practical perspective. For qualitative research and empirical data collection, saturation is usually reached within around 13 interviews (Hennink and Kaiser, 2021). Therefore, we will use this mark as an orientation on how many interviews to conduct. The interviews will build on the knowledge gathered from the desk research and will therefore be complementary in providing input on recommendations on opportunities and potential policy priorities on upholding the rule of law.

Through the chosen methodology, we intend to answer both the problem statement and the research questions by analyzing the relevant legal instruments, literature, and key informant interviews to highlight key challenges and potential areas of focus for regulatory priorities.

Combination of secondary research and interviews

Through the literature review, secondary research has already given us a comprehensive understanding of the challenges and stakeholders. Therefore, the main body of this report will focus on best practices and recommendations. Those will be based

mainly on interviews as we hope that practitioners from the field are best equipped to give us a hands-on perspective of the regulation within digital spaces. The secondary research also helped us tailor interview questions specifically to the nexus of different challenges and to comprehend the cooperation of different actors in the field. The direction this research will take, will be heavily defined by who we are able to speak to. Hence, the secondary research adapts to the arguments highlighted by the interviewees, and fills potential gaps, which have not been sufficiently covered during interviews. Furthermore, secondary research is important to lay an academic foundation before the interviews are conducted and validate findings from the interviewees in the aftermath.

8. LIMITATIONS

National and regional legislation and jurisprudence are influential in the regulation of digital spaces. However, this research project is designed to map out global trends and best practices and does not have the capacity to analyze specific national regulations and regional frameworks. Therefore, the analysis of national and regional frameworks is outside the scope of this research.

This report breaks down the international and regional legal frameworks applicable to digital spaces, focusing on hard and soft law elements. Furthermore, this report does not look into enforcement or remedies of violations of the human rights examined. Regardless of this aspect falling outside the scope of this report, it is however important for a holistic view of advancing human rights in digital spaces and should be considered by IDLO in further research.

These limitations can be overcome by IDLO in conducting further consultations with their relevant stakeholders as well as undertaking future research on this subject matter in the development of its digital innovation and rule of law programmatic framework.

9. SUMMARY OF CHALLENGES & STAKEHOLDERS

Key Stakeholders

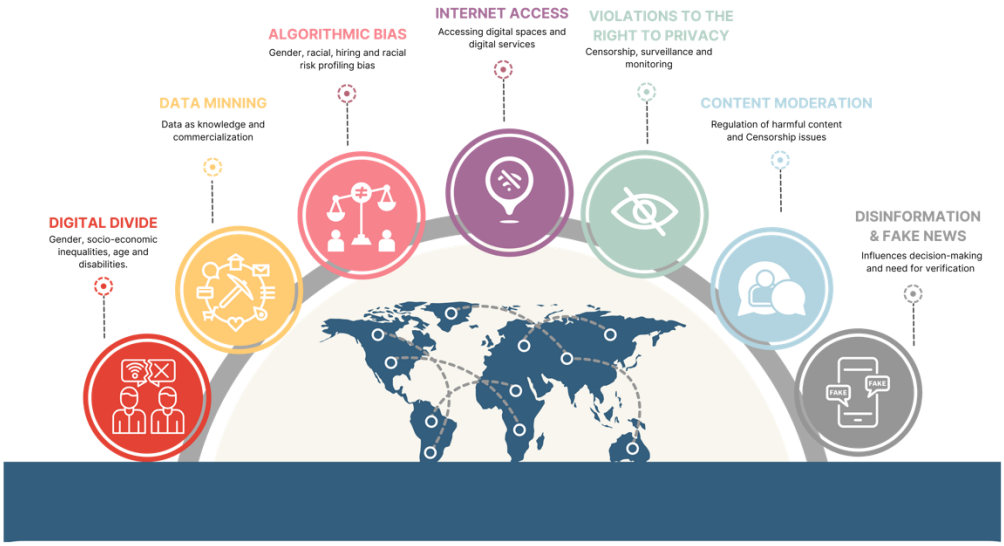
From secondary research, the research identified the key stakeholders relevant to the study and the relevant issues as illustrated below:

Figure 2: Stakeholders in Digital Spaces

Summary of Challenges in Digital Spaces

The research highlighted several key challenges including the digital divide, data mining, algorithmic bias, access to the internet, violations to the right to privacy, inadequate content moderation as well as disinformation and fake news.

Figure 3: Key Challenges of Human Rights in Digital Spaces



10. BEST PRACTICES

Best Practices in the Regulation of Digital Spaces to Promote Human Rights

This section focuses on best practices of the regulation of digital spaces outlined by academia, states, international organizations, technology companies, and civil society organizations. This section will be based on findings from semi-structured interviews and complemented with secondary research. The scheduled interviews and interview questions are included in Annex 4 of this report.

10.1 States

a) Development of unified regional instruments for digital regulation

European Union – declaration on digital rights and principles

The European Commission prepared a draft declaration on the digital rights and principles to ensure that there is a human-centred digital transformation. The aim of this draft declaration is to ensure that the rights respected in Europe are implemented both online and offline. As such, the declaration has been tabled by the European Commission and must be agreed upon by the other institutions in the EU, including the European Council and European Parliament. This is a positive move by the EU in ensuring that there is human centred regulation of the online space and ensures that no one is left behind in the current digital transformation. The EU draft declaration considers a variety of relevant themes in digital regulation including people and rights- centred digital transformation, promoting solidarity and inclusion, guaranteeing freedom of choice online, increasing public participation in the digital, upholding safety and security of individuals online, and sustainability of a digital future (European Commission, 2022).

Council of Europe - regulation of AI

Regulatory frameworks for specifically tackling algorithmic impacts exist, for instance the Council of Europe's ad hoc Committee on AI (CAHAI) has developed the Human Rights, Democracy, and Rule of Law Impact Assessment (HUDERIA) (Council of Europe, 2020). The CAHAI proposed the establishment of a transversal legally binding document, followed by the adoption of a risk classification methodology of the AI system. To this end, the committee proposed the idea of imposing a full or partial moratorium ban on AI systems that are deemed to present an “unacceptable risk” (Council of Europe, 2020). This would imply banning the use of AI systems when AI is used for mass surveillance or social scoring to determine access to essential services.

The CAHAI's proposed the HUDERIA's which hold the AI systems accountable by providing an *ex-ante* and *ex-poste* (dynamic) assessment of the potential impacts of business, policy and technology practices. Furthermore, it provides a reflexive exercise for AI developers to examine their own experiences, beliefs, judgments, and practices to question and attain the outcomes for suitable mitigation measures.

African Union and African Commission

The AU Policy and Regulation Initiative for Digital Africa is a programme developed by the African Union which aims to harmonise the policy, regulatory and legislative frameworks amongst the countries on the continent to enhance cooperation between telecommunications regulating authorities, public authorities and the civil society on the regional and continental space. Furthermore, the programme ensures that there is involvement of African stakeholders in the global internet governance debate (African Union, 2020). This regional effort is significant in narrowing the digital divide, specifically relating to access to and use of digital infrastructure in the region, in both urban and rural areas.

Furthermore, with respect to the freedom of expression, the African Commission on Human and Peoples' Rights (African Commission), developed the Human and People's Rights Declaration of Principles on Freedom of Expression in Africa (2019) covering the freedom of expression and opinion in the African region (African Commission, 2019). This is a unique regional instrument that is specific to promoting and regulation of the freedom of expression and access to and dissipation of information in Africa. In the introduction to the Declaration, the African Commission states that the Declaration takes note of developments in the current internet age. The development of this Declaration was also led by the Special Rapporteur on Freedom of expression and Access to information in Africa in close collaboration with relevant stakeholders.

Latin America and the Caribbean

The Latin America and Caribbean region have recently collaborated to define priorities in the digital transformation at a regional level through the development of the "Digital Agenda for Latin America and the Caribbean" (CEPAL, 2022). Between 16 and 18 November, 2022, the government representative of the regions, including the private sector, scholars and civil society came together to participate in a conference that aims to identify the priorities to drive digital development and transformation including its governance and regulation as well as narrowing the digital divide to ensure inclusion, cybersecurity and public participation.

Organization of American States

The Organization of American States shows collaboration of the states in the Americas in developing an agreed

standard to regulate freedom of expression in the region. OAS has developed the Declaration of Principles on Freedom of Expression which upholds the right to freedom of expression, opinion, and information. Additionally, this Declaration is imperative to tackle the challenges that the OAS member states face which limit the freedom of expression and media including murder, kidnapping, intimidation of and/or threats to social communicators (OAS, 2000). OAS also developed the institution of 'special rapporteurship for freedom of expression' which is key in efforts to ensure that there is specific focus on addressing emerging challenges related to the digital age.

b) Revamping of national laws to promote human rights in digital spaces

Strengthening digital regulation laws

In many countries across the world, digital spaces are governed by a patchwork of legislations on cybercrime, data protection, consumer protection and electronic transactions (UNCTAD, 2022). According to UNCTAD, the adoption of national legislations governing the digital spaces are as follows:

Table 1: Overview of national legislations governing digital spaces

	Legislation	Draft Legislation	No Legislation	No Data
E-transaction laws	81%	7%	4%	8%
Cybercrime laws	80%	5%	13%	1%
Data protection and privacy laws	71%	9%	15%	5%
Consumer protection laws	59%	5%	9%	27%

Source: UNCTAD, 2022

For effective government regulation of digital spaces globally, there is a need to strengthen national legislations where they exist to promote better protection of digital rights. Where the legislations are not in place or draft legislations exist, the governments should focus on putting in place strong human rights centred legislations to protect digital rights.

Strengthening National AI regulation

In many countries, regulation and legal frameworks have not caught up to the developing and fast changing AI software and do not set out rules and regulations of algorithmic impact and safe, ethical and human rights centric uses of such software. However, Canada has shown some best practice in the effective regulation of AI through algorithmic impact assessment. The Canadian Algorithmic Decision-Making Directive, which is a risk-based governance model, came into force in 2020. It consists of the Algorithmic Impact Assessment (AIA) tool which is a risk assessment tool that determines the impact level of an automated decision-making system. The AIA tool acts as a checklist for enabling accountability since it contains a list of questions regarding the why, what and how a system will be built in order to minimise errors and avoid risks, including what kind of human interventions and monitoring it will require (Government of Canada, 2018).

c) Internationally agreed frameworks on digital regulation

There are existing internationally agreed frameworks including policies that currently regulate certain digital spaces. For example, the OECD Recommendation on Enhancing Access to and Sharing of Data is an internationally agreed policy by several states on how to use all types of data across sectors whilst protecting the rights of the owners (OECD, 2022).

Several NGOs including Equality Now and Women in AI have championed the development and adoption of an internationally agreed set of principles specifically governing digital rights, known as the Universal Declaration on Digital Rights. This would be a significant development in ensuring that the existing rights under the Universal Declaration on Human Rights and other human rights instruments are supplemented and capable of stronger implementation in the digital age and would strengthen international cooperation in governance of digital rights.

According to a former French Ambassador interviewed for this project, there is a need for a global cooperation model on digital regulation addressing all aspects of technology that needs cross-border regulation including artificial intelligence, whilst promoting human rights in addressing issues such as the existing digital divide (Interview 2, 2022).

10.2 International Organizations

The UN has taken positive steps in the protection of digital rights through the development of the UN Global Digital Compact (GDC) to build a set of internationally agreed principles (UN, 2022). In this, the UN has ensured that it prioritizes the improvement of the existing architecture for digital regulation and cooperation, which has often been disjointed and lacks proper procedures. Currently, the Internet Governance Forum promotes international cooperation on issues concerning the internet and meets severally in the year to ensure this agenda is implemented to become more effective (UN, 2022). In undertaking the development of the GDC and improving on the existing digital architecture, the UN has highlighted the potential of digital technology not only bringing about positive change but also worsening existing inequalities. As such, the UN indicated that it is a priority to cooperate globally to protect and promote human rights and human well-being in technology governance whilst ensuring development of effective institutional frameworks, promotion of digital security, digital trust as well as inclusivity in the digital economy and society at large (UN, 2020).

The UN Habitat has also developed a draft Framework for Digital Rights, which is now open for feedback from stakeholders, that is specific to the context of city governments (UN HABITAT, 2022). This Framework governs how cities can tackle issues of their digitalisation and connectivity such as the existing digital divide while aiming to increase the number of people having access to the internet through human rights centred processes of addressing connectivity needs, digital inclusion and capacity building.

Furthermore, there are some recommendations made by international organizations that are specific to AI, such as guidelines from UNESCO (2021) which could potentially alleviate some of the negative consequences of AI. The UNESCO guidelines strongly encourage that developers and providers of AI technologies do ethical impact evaluations to guarantee that their innovations take into account the socio-economic impacts of their inventions while also protecting individuals' rights. The recommendations encourage member states to ensure that the harms caused by AI systems are addressed, and remedial actions are taken. In addition, it makes a number of recommendations highlighting how member states can improve their governance and monitoring mechanisms by introducing different methods, including certifications, self-assessments, developing international standards, development and access to digital ecosystems for ethical development.

UNDP has put in place a strategic foresight office which works with country programmes, in both the medium and long term, to determine

risk indicators and factors of uncertainty with regards to the digital domain (Interview 5, 2022). In this role, it looks at governance around technology and embracing all types of technology while foreseeing the challenges that may come up in the utilisation of such technologies. UNDP therefore considers strategic foresight as a policy making tool to assist the various regulatory stakeholders in making collective informed decisions (UNDP et al, 2014). Thus, international organizations can consider putting in place strategic foresight frameworks to assist them in furthering their agenda regarding human centric regulation of digital technologies.

10.3 Civil Society Organizations

Amnesty International has identified encryption as an effective means to protect privacy and freedom of expression online, making communication and data safe. Encryption can protect individuals from government surveillance and data abuse through hackers. As technology companies pledge human rights commitments, they differ in their implementation of encryption. Amnesty ranked the different technology companies in their effective implementation of encryption of the digital services they are offering (Table 2). Thereby, Amnesty assumes the role to check on technology companies who are important de-facto regulators. By ranking these technology companies against each other, Amnesty builds pressure among them in the eye of their reputation and further business opportunities (Amnesty, 2016).

Table 2: Ranking of technology companies' encryption level in messenger services

Ranking position	Company	Instant messaging services	Replied to Amnesty's request for information?	Overall score /100
1	Facebook	FB Messenger, WhatsApp	Yes	73
2	Apple	iMessage, FaceTime	Yes	67
3	Telegram	Telegram Messenger	Yes	67
4	Google	Allo, Duo, Hangouts	No	53
5	Line	Line	Yes	47
6	Viber Media	Viber	Yes	47
7	Kakao Inc	KakaoTalk	Yes	40
8	Microsoft	Skype	Yes	40
9	Snapchat	Snapchat	Yes	26
10	Blackberry	Blackberry Messenger	No	20
11	Tencent	QQ, WeChat	No	0

Human Rights Watch campaigns for the development of a multistakeholder internet governance, which abandons the current State centric model of multilateral governance. Concepts like internet sovereignty, promoted by China, would be devastating for international human rights protection. The functioning of the internet is dependent on the inclusion of diverse stakeholders and can only be successful if they understand that protection of human rights means protecting national security, and not threatening it (Human Rights Watch, 2014). Additionally, a former French Ambassador (Interview 2, 2022) echoed similar statements and mentioned that a democratic character of a State should be accompanied by a framework democratic governance of the internet. He also emphasised that multistakeholder internet governance is subject to the democratic and pluralistic nature of a State. If a State is non-democratic, then it is very unlikely that it will adopt a multi stakeholder approach.

Article 19 and the Danish Institute for Human Rights have developed a human rights assessment tool, a publicly available methodology designed to help providers of digital services to evaluate their impact on human rights (Article 19 and The Danish Institute for Human Rights, 2020).

Furthermore, initiatives like the Open Government Partnership (OGP), engaging with 78 countries worldwide, influences policy discussion putting more emphasis on how to leverage technical possibilities for governments to communicate and share information with citizens to safeguard the right to access to information (DIA, 2020). For instance, such a partnership project in Latvia established a common online platform to inform and engage citizens on legislative processes (OGP, Latvia). In Colombia an interactive website and call center was developed to ensure the access to government information for deaf and blind people (OGP, Colombia).

According to Emma Gibson, CEO of Women in AI and Campaign Leader for Universal Digital Rights at Equality Now, a global approach to the regulation of human rights in digital spaces is needed. This means using the existing human rights framework and developing an approach all countries could sign up to. The existing situation of voluntary self-regulation of technology companies is not working sufficiently, rather they need to be overseen formally by governments (Interview 4, 2022). Durach, Bargaoanu and Nastasiu (2020) advocate for a co-regulatory framework in countering human rights challenges on digital platforms, particularly disinformation. This would entail setting up of the principles and objectives of the co-regulatory framework at a supranational level, followed by contributions from the industry (co-regulatory bodies from the industry). Therefore, for instance, a co-regulatory approach would focus on developing a framework for cooperation between national and EU-level government agencies, online platform providers,

media organizations, researchers, and other stakeholders.

Emma Gibson (Interview 4, 2022) also advocates that special emphasis should be given to mechanisms that ensure feminist and inter-gender inclusion, as the internet is exacerbating existing inequalities. Similarly, even the methods proposed by different scholars for "de-biasing" gender bias in machine learning have been very extensive and broad. For example, Luka and Millette (2015) suggest adopting an intersectional feminist practice of "ethics of care" for conducting ethical research in the era of big data. They encourage researchers to analyze one's own actions to identify biases to prevent it from being exacerbated in textual scholarly data.

In contrast, Aarathi Krishnan (Interview 5, 2022), Strategic and Foresight Advisor at UNDP, pointed out that ethics is rather hard to regulate as it is often premised on moral obligations. She referred to ethics as a "Western concept" which is often cast as ethics washing and in this context based on the assumption that all women have similar backgrounds and experiences. She pointed out that developers should go beyond the gender binaries and be more inclusive to reduce bias at a design level. Secondly, scholars like Luka and Millette (2015) also advocate for the adoption of a "feminist materialist speculation" as a method of ethical research. Their argument is based on the idea of situated knowledge by Harraway (1988) and sets a foundation for a speculative methodology of doing research. Their proposal urges researchers to consider a contextualized approach for speculating the social relations imbricated in data and datasets. Furthermore, Joyce et al. (2021) proposes the employment and creation of "AI socio-technical systems" as an intersectional sociological framework for investigating the inequalities in algorithms, codes, and data. The deployment of AI socio-technical systems as a framework of research has the potential to further the discussion on unequal practices of the AI systems and give an account for the social realities that are embedded in data. This approach can account for global histories of slavery, patriarchy, white supremacy, and capitalism, as well as the ways in which the contemporary and historical iterations of these systems are reproduced, aggravated and resisted in digital systems.

Additionally, Leavy, O'Sullivian & Siapera (2020) argue that while reasoning about bias, we need to involve those who might be directly impacted by the algorithmic decisions. They emphasize the concept of "democratization of data" and propose interrogating the socio-political ramifications of ethical data gathering practices. Data collection for machine learning algorithms raises important questions about how to balance the socio-political effects of data collection on different groups in society.

The principle of non-discrimination shall define how existing human rights norms

should be applied. A huge challenge for individuals and civil society is to seek redress because offences and technology companies often have a cross border dimension. As the role of civil society is to pressure and push actors to go faster and further, the current development at the UN level establishing a technology envoy to the Secretary General and the pursuing the Global Digital compact, is an opportunity for civil society organizations like Women in AI and Equality Now to influence the dialogue at the international decision-maker level. Furthermore, civil society organizations have used judicial processes to test the boundaries of existing regulation (Interview 4, 2022). For instance, on the activists' initiative, the Dutch courts banned an algorithm used by the government to detect possible social welfare fraud (Algorithmwatch, 2020).

Tackling the digital divide with respect to access and use has become very critical. A quantitative study conducted by Mehra, Sikes, and Singh (2019) (Figure 4) illustrates how the technology use and community involvement in Southern and Central Appalachian (SCA) rural libraries was used as a means of overcoming marginalisation for bridging the rural digital divides that have historically existed in that area. The study was based on a qualitative content analysis of contributions received from 15 rural librarians through semi-structured interviews and three participants in each of five focus groups between 2017 and 2018. The rural SCA librarians offered a range of technological activities as can be seen in the figure below. These comprised both individual and group-centred activities. Their services included both computer and internet related access as well as technology training classes, workforce development programming as well as access to online resources, electronic databases, etc. The outcome of such an exploratory model of community engagement was extremely successful since many respondents provided the feedback that by providing access to online knowledge, the librarians were able to promote a skilled workforce and adequately help people in developing technical skills to find information online.

The Swiss Digital Initiative, as a non-profit organization, has issued a Digital Trust Label to denote the trustworthiness of digital services in non-technical language. It entails a mechanism for cases of non-compliance where the label is revoked and publicly announced. To safeguard privacy, building trust in digital services can be a challenge. Non-profit organizations can be important mediators between users, and technology companies or governments providing digital services. According to Nicolas Zahn, designation from the Swiss Digital Initiative, non-profit organizations play an important role in developing ethical and responsibility standards in parallel to the technological innovation process (Interview 3, 2022).

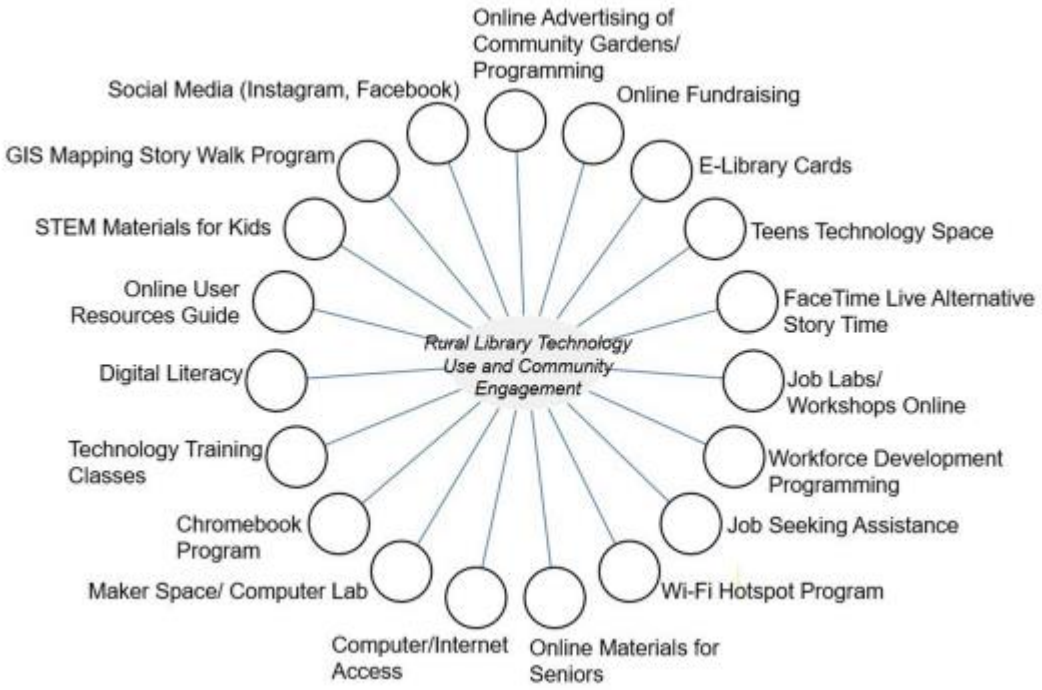


Figure 4: **Technology-related community engagement projects in SCA rural libraries**

Source: *Mehra, Sikes, and Singh, 2019*

10.4 Technology Companies

Technology companies have released official human rights statements committing to the UN Guiding Principles on Business and Human Rights (UN Working Group on Business and Human Rights, 2011) and the Global Network Initiative (2008). Microsoft's statement is even available in a great majority of languages, even local (Microsoft Global Human Rights Statement).

Microsoft has made a Human Rights Impact Assessment Template publicly available to evaluate the compatibility with AI products, which other companies can use as a best practice (Microsoft, 2022). In fact, Microsoft has a framework in place for building AI responsibly. It aims to break down principles like accountability into comprehensive parameters, e.g., impact assessment, data governance, and human oversight. It formulates privacy and inclusiveness as core values, however, does not mention human rights explicitly (Microsoft, 2022).

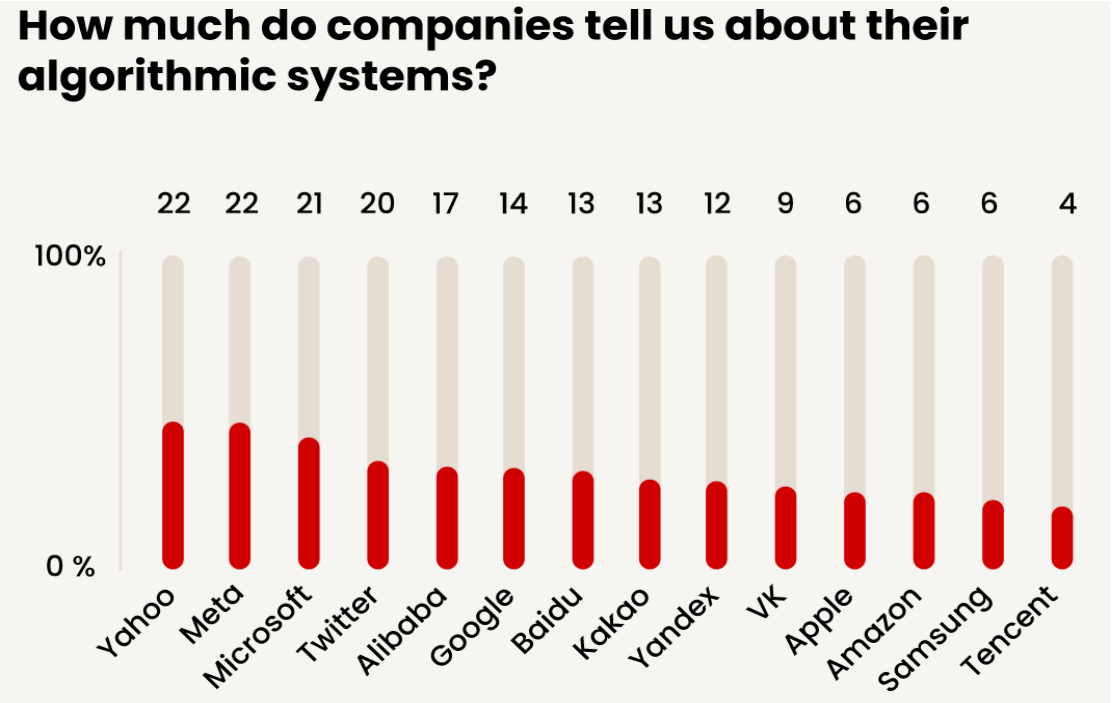
Likewise, Google has published Guidelines on the Responsible Development of AI. Although this step is acknowledged as important, it still falls short to fully comply with the human rights framework, particularly freedom of expression and right to privacy. Due to the lack of clear definitions, the scope of the guidelines remains uncertain. The paper employs review mechanisms but does not connect it to international standards of transparency and accountability. Furthermore, Google openly questions

whether data protection should apply across borders, as explicitly demanded by the GDPR. Moreover, Google guidelines have been criticized as it outlines few meaningful engagements with multi-stakeholders (Article 19, 2018).

In July 2022, Meta released its Human Rights Report. It recognizes that human rights in digital spaces extend beyond the user itself. It establishes a trusted partner program bringing over 400 NGOs and human rights defenders from over 100 countries to the table, although clarification on the exact process is missing. Yet, it has been criticized that the report does not acknowledge that Meta's business model is to infringe on the right to privacy to moderate advertisements to its profit. Lastly, the fact that the human rights policy team was only staffed with four full time members in 2021, seems not enough (Ranking Digital Rights, 2022). Additionally, Amnesty points at a lack of transparency as Meta rejected to publish the full report in India (Amnesty International, 2022).

In considering AI human rights impact assessment, a major factor is technology companies making their algorithms transparent and thereby revealing the extent of control users have. The figure below illustrates the current ranking among technology companies regarding AI transparency (Ranking Digital Rights, 2022).

Figure 5: Ranking of technology companies' AI transparency



Source: Ranking Digital Rights, 2022

Regarding internal policies, technology companies have noticed the existing threat technology poses to human rights. Some exemplary policies that have been adapted, are the incorporation of translations into sign language, improving accessibility programs in response to discrimination issues in facial recognition, or increasingly employing women and historically disadvantaged people at technology companies. Furthermore, internal training on AI and freedom of expression, guided by recent court judgements, are conducted. Also, technology companies increasingly invest in cyber protection. Yet, the perception of their own regulation power seems to be moderate when stating that technology companies are guided by country specific laws and could only choose whether to do business or not in certain countries (Interview 1, 2022).

In 2022, companies have increased their engagement with multiple stakeholders and civil society but are not prioritising remedy mechanisms for human rights violations. Furthermore, there has long been a discrepancy between the human rights awareness of technology companies in the Global North and the Global South. Overall, there is a trend that companies are increasingly aware of human rights in technology and feel urged to position themselves on this issue (Ranking Digital Rights, 2022). Freedom of speech and right to privacy seem to be of most concern to technology companies.

11. RECOMMENDATIONS

IMPROVED DIGITAL GOVERNANCE

- **Development of human rights centric internationally agreed minimum standards for digital governance by multi stakeholders** including technology companies, states, civil society, and private actors. A common understanding of such standards would be specifically tailored to govern rights in the digital age that are not adequately addressed by the existing international human rights framework. They would put in place a minimum threshold to tackle challenges such as dominant self regulation by technology companies, challenges to the right to privacy (data-mining, surveillance and exploitative data commercialization) and freedom of expression, non-inclusive and discriminatory online services and applications used by states and private actors. The agreed minimum standards would bridge the gaps in existing international and state regulatory frameworks.

- **Establishment of a national co-regulatory approach for digital governance** which would entail a framework of cooperation between national and supranational agencies, tech companies, online platform providers, media organizations, researchers, and other stakeholders. This would entail the adoption of national principles, in line with the internationally agreed minimum standards, and the creation of a regulatory body tasked with human rights centred approach to regulation. A co-regulatory approach at a national level would address state centric challenges associated with freedom of expression such as content moderation, censorship, disinformation, and fake news.

NARROWING THE DIGITAL DIVIDE

- **Establishment of community engagement programs initiated by local authorities for bridging the digital divide** when it comes to socio-economically disadvantaged, women and girls, and people in rural areas through digital upskilling of community members and increased access to technological devices and infrastructure like computer laboratories, mobile phones, internet, etc.

- **Collaboration of civil society and governments to promote the inclusive access of governmental services** such as providing the services in multiple languages and facilitating disability friendly tools to online governmental services.

MITIGATING ALGORITHMIC BIAS

- **Technology companies, developers and users (such as governments, public and private actors) of algorithmic softwares should implement a bias impact assessment mechanism** to probe, alert and address any potential biases and human rights violations that can result from algorithmic decisions. As a best practice, algorithmic creators should consider a set of initial assumptions about the algorithmic impact prior to its development and execution. Users applying such mechanisms would help address biased challenges arising from algorithmic softwares in criminal justice systems, welfare schemes and for credit scoring.

- **Technology companies and other developers should develop algorithmic softwares based on globalised data**. The big data used for training algorithmic decisions can most often perpetuate existing biases due to a) under-representation of data and/ or b) biased data-sets. To mitigate the use of such biased algorithmic softwares, diverse global data-sets should be utilised to ensure that the training of AI software is more inclusive and non-biased. Additionally, efforts must be taken to increase the scrutiny of the data and the processes used to generate discriminatory algorithmic models. This can be done through regular impartial independent auditing (of data-sets), by allowing external parties to examine data-sets and their results, and wherever possible making it open source and easily available and accessible to the public for scrutiny.

LIMITATIONS OF THE RECOMMENDATIONS

The above recommendations can help advance the rule of law and human rights in digital spaces. However, we note that there are cross-cutting limitations to the recommendations mentioned above. Firstly, it would be a challenge for states to develop internally agreed minimum standards on digital governance due to long winded negotiations and diverging interests and interpretations. Secondly, such recommendations to the relevant stakeholders, specifically private actors including technology companies, are difficult to adopt and implement due to lack of good-will which is overweighed by profit maximization motivations. Thirdly, the establishment of independent auditing bodies, of community engagement programs, diversifying existing policies and projects with a view to promoting inclusivity is limited due to funding constraints. In adopting such recommendations, civil society can play a key role in lobbying for prioritisation of funding, awareness raising of human rights violations, promotion of good-will, pushing for agreed common standards, and acting as agents of change by relying on judicial systems and holding states accountable to comply with international standards.

12. CONCLUSION

This report aimed to map out current challenges to the rule of law and human rights in digital spaces and formulate recommendations for relevant stakeholders to address these challenges. Focusing on the rights such as freedom of expression, access to information, privacy and non-discrimination, we found that the digital divide, data mining, algorithmic bias, internet access, privacy violations, content moderation, and disinformation and fake news are the most pressing challenges in digital spaces.

While there is the international human rights framework including the UDHR, ICCPR, and ICESCR, and emerging soft law, as well as regional legal frameworks, there are significant gaps in the regulation of digital spaces that could live up to the standards set out by the international human rights framework. Often, these gaps are filled by the self-regulation of technology companies, as well as non-binding guidelines by the relevant regulating entities. However, such efforts of making digital spaces human rights centric are insufficient.

International organizations, states, private sector actors, civil society, and technology companies are key actors in the regulation of digital spaces. Therefore, relevant stakeholders need to collaborate to improve digital governance, narrow the digital divide, and mitigate algorithmic biases.

Improving digital governance entails the development of international human rights centric minimum standards for the governance of digital spaces. Thereby, it is important to have this multistakeholder base to develop a common understanding and bridge the gaps in national and international regulation. Furthermore, improving digital governance means establishing a national co-regulatory approach, which would adopt national principles in line with internationally agreed standards, being informed by multiple stakeholders.

Narrowing the digital divide can be achieved through community engagement programs initiated by local authorities leading to technical upskilling of socio-economically disadvantaged groups. In addition, partnerships between civil-society actors and governments is key to designing more inclusive and accessible online government services.

Mitigating algorithmic biases obliges technology companies, developers and users of algorithmic software to implement bias assessment mechanisms prior to its development and execution. Furthermore, the development of algorithmic software needs to be based on global data, to mitigate discrimination biases by AI. To ensure transparency, AI should wherever possible be an open source available to the public for scrutiny.

Although the implementation of these recommendations highly depends on the meaningful cooperation of diverse stakeholders, it is important to highlight the crucial role that civil society can play in enforcing accountability of technology companies and other regulatory actors.

13. BIBLIOGRAPHY

Access Now (2018). A user guide to data protection in the European Union.

African Commission on Human and Peoples' Rights. Declaration of Principles on Freedom of Expression and Access to Information in Africa.

African Union. AU Policy and Regulation Initiative for Digital Africa (PRIDA).

Algorithmwatch (2020). How Dutch Activists got an invasive fraud detection algorithm.

Alvarez, Hall, and Trechsel (2009). Internet Voting in Comparative Perspective: The Case of Estonia. *Political Science and Politics. 42(3).* 497-505.

Amnesty International (2016). For your Eyes Only? Ranking 11 Technology Companies on Encryption and Human Rights.

Amnesty International (2019). Surveillance Giants: How the business model of Google and Facebook threatens human rights.

Amnesty International (2021). Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal.

Amnesty International (2022). Meta's Human Rights Report ignores the real threat the company poses to human rights worldwide.

Article 19 (2018). Google: New Guiding Principles on AI show progress but still fall short on human rights protections.

Article 19 (2019). Tackling gender inequality through access to information.

Article 19 & The Danish Institute for Human Rights (2020). Registry Human Rights Assessment Tool.

Article 19 (2021). US: A Capitol riot and Big Tech takes as stand: but is this the one we want?

Asia-Pacific Economic Cooperation (2022). What Is the Cross-Border Privacy Rules System.

Bellovin, Hutchins, Jebara, and Zimmeck (2013). When enough is enough: Location tracking, mosaic theory, and machine learning. *NYUJL & Liberty*, *8*, 556.

Björksten, Wentworth, Cheng, and Rosson (2022). Taxonomy of a shutdown: 8 ways how governments restrict access to the internet, and how to #KeepItOn. Access Now.

Calzada (2021). The right to have digital rights in smart cities. Sustainability, 13(20), 11438.

Council of Europe (2020). Ad hoc committee on artificial intelligence (CAHAI). Feasibility Study.

Davaki (2018). The underlying causes of the digital gender gap and possible solutions for enhanced digital inclusion of women and girls. FEMM: Women's Rights and Gender Equality.

Democracy in Africa (DIA) (2020). How to ensure digital access to information in Africa.

Durach, F., Bargaoanu, A., & Nastasiu, C. (2020). Tackling disinformation: EU regulation of the digital space. Romanian Journal of European Affairs, 20(1), 5-20

Dwoskin, and Timberg (2021). Misinformation dropped dramatically the week after Twitter banned Trump and some allies. The Washington Post.

ECLAC. Digital Agenda for Latin America and the Caribbean for 2024.

Eubanks (2018). The digital poorhouse. *Harper's Magazine*.

European Commission. European Digital Rights and Principles.

Esposito (2017). Algorithmic memory and the right to be forgotten on the web. Big Data & Society, 4(1).

Fjeld, Achten, and others (2020). Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center Research Publication, (2020-1).

Global Centre for Public Service Excellence and UNDP (2014). Foresight as a Strategic Long- Term Planning Tool for Developing Countries.

Google (2018). Responsible Development of AI.

Government of Canada (2018). Algorithmic Impact Assessment (AIA).

Government of Germany and Government of the United Arab Emirates (Co-Champions). Recommendation 5A/B: Options for the Future of Global Digital Cooperation.

Hennink, and Kaiser (2021). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine.

Human Rights Watch (2014). Human Rights in the Digital Age.

Jacobs (2021). Moving from Access to Accessibility: The Deception of the Digital Divide in Development. UNDP South Africa.

Joyce, K., Smith-Doerr, L., Alegria, S., Bell, S., Cruz, T., Hoffman, S. G., Noble, S. U., & Shestakofsky, B. (2021). Toward a Sociology of Artificial Intelligence: A Call for Research on Inequalities and Structural Change.

Kleinberg, J., Lakkaraju, H., Leskovec, J., Ludwig, J., & Mullainathan, S. (2018). Human decisions and machine predictions. The quarterly journal of economics, 133(1), 237-293

Lawrence Neuman (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Pearson Education Limited.

Leavy, S., O'Sullivan, B., & Siapera, E. (2020). Data, power and bias in artificial intelligence. arXiv preprint arXiv:2008.07341.

Luka, M. E., & Millette, M. (2015). (Re) framing Big Data: Activating Situated Knowledges and a Feminist Ethics of Care in Social Media Research', Social Media+ Society, April 2018. International Journal of Social Research Methodology, 18(2), 193-207

Ma. Dolores C. Tongco (2007). Purposive Sampling as a Tool for Informant Selection. Ethnobotany Research and Applications, 5:147-158.

Mathiesen (2014). Human rights for the digital age. *Journal of Mass Media Ethics*, *29*(1), 2-18.

Mendel, Puddephatt, and others (2012). Global survey on internet privacy and freedom of expression. UNESCO.

Meta (2022). Meta Human Rights Report. Insights and Actions 2020 – 2021.

Microsoft (2022). Microsoft Responsible AI Impact Assessment Template.

Microsoft (2022). Microsoft's framework for building AI systems responsibly.

Nawaz (2019). How Far Have We Come With The Study Of Artificial Intelligence For Recruitment Process.

Neuman (2022). Promoting Gender Equity in the Right of Access to Information. UNESCO.

Nolasco, and Micek (2018). Access Now responds to Special Rapporteur Kaye on 'Content Regulation in the Digital Age. Access Now.

OAS (2000). Declaration of Principles on Freedom of Expression.

OECD. Data governance: Enhancing access to and sharing of data.

OHCHR (2019). United Nations Special Rapporteur on the promotions and protection of the right to freedom of opinion and expression. Freedom of Expression and Elections in the Digital Age.

Oliva (2020). Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression. Human Rights Law Review, 2020, 20, 607–640

Open Government Partnership (OGP). Actions for Transparent and Accountable Digital Governance.

Open Government Partnership (OGP). Colombia: Access to Information for People with Disabilities (CO0033).

Open Government Partnership (OGP). Latvia: e-Legal Services (LV0029).

Privacy International and ARTICLE 19 (2018). Privacy and freedom of expression in the age of artificial intelligence.

Prates, Avelar, and Lamb (2020). Assessing gender bias in machine translation: a case study with google translate. Neural Computing and Applications, 32(10), 6363-6381.

Ranking Digital Rights (2022). Key Findings from the 2022 RDR Big Tech Scorecard.

Ranking Digital Rights (2022). Meta's First Human Rights Report: The Good, the Bad, and the Missing.

Sander (2020). Freedom of expression in the age of online platforms: the promise and pitfalls of human rights-based approach to content moderation. Fordham International Law Journal, 43(4), 939-1006

Swiss Digital Initiative. The Digital Trust Label.

UNCTAD. Summary of Adoption of E-Commerce Legislation Worldwide.

UNDP Practice Note (2003). Access to Information.

UNDP Ukraine. Digital, Inclusive, Accessible: Support to Digitalisation of Public Services in Ukraine (DIA Support) Project.

UNDP Ukraine (2022). Ukraine highlights effort to close digital divide for people with disabilities during the New York conference.

UNESCO (2021). *UNESCO: Recommendation on the ethics of artificial intelligence*.

UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3.

UN HABITAT (2022). Digital Rights Governance Framework: Concept Draft Open for Feedback.

United Nations, Office of the Secretary General's Envoy on Technology. Global Digital Cooperation.

United Nations (2020). Report of the Secretary General, Roadmap for Digital Cooperation.

Universal Rights Group (2021). Placing Digital Technology at the Service of Democracy and Human Rights. Outcome of the Second Digital Democracy Dialogue. 16-17 November 2021.

Walker (2016). Face recognition app taking Russia by storm may bring end to public anonymity. Guardian.

Zuiderveen (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. The International Journal of Human Rights, 24(10), 1572-1593.

14. ANNEXES

Annex 1: Summary of Human Rights Instruments regarding Digital Spaces

HUMAN RIGHT	HARD LAW	SOFT LAW
Freedom of expression, opinion and access to information	**Article 19 of the ICCPR** 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.	**Article 19 of the UDHR** Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. **The Rabat Plan of Action** The Rabat Plan of Action suggests a high threshold for defining restrictions on freedom of expression, incitement to hatred, and for the application of article 20 of the ICCPR. It outlines a six-part threshold test taking into account (1) the social and political context, (2) status of the speaker, (3) intent to incite the audience against a target group, (4) content and form of the speech, (5) extent of its dissemination and (6) likelihood of harm, including imminence. The **UN Digital Road Map** which focuses on digital cooperation among stakeholders.

HUMAN RIGHT	HARD LAW	SOFT LAW
	Article 20 of the ICCPR 1. Any propaganda for war shall be prohibited by law. 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.	The **UN Interagency Dialogue on Disinformation and Data Transparency** which provides guidance on digital rights in countering disinformation, data protection, and data privacy. The **Human Rights Committee General Comment Number 34** which provides further guidelines on the implementation of Article 19 of the ICCPR on the freedom of opinion and expression. The **African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa** covers the freedom of expression and opinion in the African region.
Right to Privacy	**Article 17 of the ICCPR** 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.	**Article 12 of the UDHR** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

HUMAN RIGHT	HARD LAW	SOFT LAW
	AfCFTA Protocol on e-Commerce and the African Union Convention on Cyber Security and Personal Data Protection which provides a mechanism to address cyber security and personal data protection in the African region.	
Freedom from discrimination	**Article 26 of the ICCPR** All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. **Article 3 of the ICESCR** The States Parties to the present Covenant undertake to ensure the equal right of men and women to the enjoyment of all economic, social and cultural rights set forth in the present Covenant.	**Article 7 of the UDHR** All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

Annex 2: Workplan

WORKPLAN

Task	Beginning of Task	Deadline	Team Member
Literature Review Critically analyzing numerous published body of knowledge through summary, classification, and comparison of prior research studies, reviews of literature, and theoretical articles.	April 2022	15th June 2022	Ikran, Meike, Samridhi, Zak
Inception Report		8th July 2022	Ikran, Meike, Samridhi, Zak
Report Writing- Part 1 Finalizing literature view, incorporating feedback and summarizing findings.	15th August 202	14th October 2022	Ikran, Meike, Samridhi, Zak
Interviews Compilation of a list for potential interviews. Conducting semi-structured interviews with relevant stakeholders from the digital spaces and human rights domain.	15th October 2022	27th October 2022	Ikran, Meike, Samridhi
Preliminary Report		28 October 2022	Ikran, Meike, Samridhi
Interviews - Part 2	29th October 2022	mid-November 2022	Ikran, Meike, Samridhi
Report Writing- Part 2		End of November 2022	Ikran, Meike, Samridhi
Final Draft and Submission		2 December 2022	Ikran, Meike, Samridhi

Annex 3: Scheduled Interviews and Interview Questionnaire

A. Scheduled Interviews:

	Interviewee	Organization	Date/Time
Interview 1	Technology Company	Technology Company	07.11.2022
Interview 2	Former French Ambassador	N/A	08.11.2022
Interview 3	Nicolas Zahn	Swiss Digital Initiative	08.11.2022
Interview 4	Emma Gibson	Women in AI / Equality Now	14.11.2022
Interview 5	Aarathi Krishnan	UNDP Regional Bureau for Asia and the Pacific	21.11.2022

B. Interview Questionnaire:

All interviewees:

1. How would you define digital spaces and digital services?
2. What is your understanding of human rights in digital spaces? Are there digital rights as such or merely human rights applied in digital spaces?
3. Looking at the human rights relevant to digital spaces such as freedom of expression, right to privacy, access to information and freedom from discrimination– what are those that interest you the most and why? Which one do you regard the most important? How do these human rights relate to each other?
4. What do you think are the key challenges to the use of digital spaces or services from the perspective of the organization you are representing?
5. In what realm should digital spaces be regulated? In the international arena, the national level, or within a specific issue domain?

CSOs/ NGOs/ IOs/Academic Scholars:

6. Do you believe there is an emergence of digital rights, if so, what do they include?
7. Do you think the current human rights frameworks are sufficient to govern digital rights?
8. What are best practices your organization can offer in influencing the regulation of digital spaces?

9. Regarding the regulation of digital spaces, how is the cooperation between your organization and other relevant actors? What are the dynamics between private and public actors?
10. What programs has your organization in place to ensure the inclusion of vulnerable and marginalized people, such as targeting the digital divide?
11. What are the most pressing issues regarding the digital gender divide and what steps must be taken to tackle them?

CSOs/ NGOs:

12. What are best practices for the regulation of digital spaces, where civil society organizations have filled existing regulation gaps to ensure the protection of human rights?
13. What role can NGOs play in advocating for the protection of human rights in digital spaces?
14. How can NGOs and civil society influence international regulation of digital spaces that incorporate their interests?
15. What would be the three most important measures you would recommend state regulators to safeguard the protection of human rights in digital spaces?

Private Sector (Technology Companies):

16. What do you think are the key challenges to the use of digital spaces or services?
17. What regulatory frameworks does [company] put in place to safeguard human rights in the digital space - specifically on right to privacy; freedom of expression; access to information and freedom from discrimination?
18. What institutional frameworks does [company] have in place to enforce regulatory practices/ policies within the organization?
19. Other paramount issues which cannot be separated from the internet are freedom of expression and access to correct and trustworthy information. Whereas the internet greatly facilitates ways to express ourselves and the diversity of information available, it is also true that some stakeholders have the power to ban, remove or distort online content according to their interest. How should we draw the line between information worth sharing and that to be banned/censored? And who are those entitled to do so?