

Tech giants and human rights: Investor expectations



© Bryn G Jones



**THE DANISH
INSTITUTE FOR
HUMAN RIGHTS**

Introduction

Information technology is embedded in global society and used daily by billions of people. The internet, personal electronic devices and social media are intrinsic to our economic and social future and offer important opportunities to tackle social and sustainability challenges. Yet concern at tech giants' negative human rights impacts is growing and society's trust in them is being corroded. Jeopardising tech giants' social license to operate, this also carries significant business and investment risks.

Tech giants' human rights impacts range widely. Besides workforce and other supply chain issues, they include impacts linked to the gathering, use and commercialisation of personal data; facilitating the spread of hate speech, misinformation, political extremism, terrorism, electoral manipulation and the suppression of democratic dissent; the impacts of content moderation and encryption; discrimination and other human rights abuses resulting from algorithmic bias; and impacts on at-risk groups including children and human rights defenders. At system level, further impacts relate to concentration of wealth and reinforcement of inequalities, large-scale tax avoidance and its consequences for public revenues, economic instability and criminality linked to cryptocurrencies, for example. Many such issues have assumed new dimensions in the context of the COVID-19 pandemic.

Regulators face difficulties in addressing such risks and securing compliance by powerful tech giants whose activities are dynamic, diversified, transnational and technically complex. In many cases, root causes of risks to human rights go beyond individual products or services to implicate tech giants' business models, corporate governance and incentives structures, as well as the effects of dominant market positions that assume, but also transcend, the decisions and conduct of individual corporations.

These investors' expectations of tech giants on human rights were developed by the Swedish Council on Ethics of the Swedish national pension funds. Analysis of the context for the expectations was developed in collaboration with the Danish Institute for Human Rights. The expectations are primarily directed at the boards of tech giants and intended to serve as a foundational building block for investor interaction with tech giants on human rights.

Tech giants and human rights: Investor expectations

Introduction	2
Tech giants and human rights: Investor expectations	4
Context for the expectations	6
1. Purpose, outline and scope	6
2. Business and human rights standards	7
2.1. Human rights: the corporate responsibility to respect and due diligence	7
2.2. Tech-specific laws and guidance.....	8
2.2.1. Government regulation.....	8
2.2.2. Human rights bodies	8
3. Tech giants: Selected human rights risks	9
3.1. Human rights to privacy and data protection.....	9
3.1.1. Tech giants’ collection, processing and use of personal data.....	10
3.1.2. Profiling and automated decisions	11
3.1.3. Encryption and anonymity.....	11
3.1.4. Government access to platform data	11
3.2. Human right to freedom of expression	12
3.2.1. Internet access	12
3.2.2. Internet shutdowns.....	12
3.2.3. Illegal content.....	12
3.2.4. Legal content and “community standards”	13
3.2.5. Automated content filters.....	13
3.2.6. Automated content selection	13
3.2.7. Terrorism and violent extremism.....	13
3.3. Elections, public and political discourse	14
3.3.1. Disinformation	14
3.3.2. Political advertising and user profiling.....	14
3.3.3. Conflict-affected areas and non-democratic states.....	15
3.4. Discrimination and at-risk groups.....	15
3.4.1. Hate speech.....	15
3.4.2. Artificial intelligence.....	16
3.4.3. Impacts on vulnerable and at-risk groups.....	16
Further resources	17

Tech giants and human rights: Investor expectations

- Tech giant boards should ensure that the company has a policy to respect human rights and that relevant measures are integrated into corporate business strategy, risk management, and reporting.
- Tech giant boards should ascertain that the ensuing human rights responsibilities are clearly defined within the organisation and they should effectively guide, monitor, and review company management in carrying out these efforts.
- Tech giant boards should be transparent about the topics raised in this document. Appropriate and timely reporting, as well as measurable data, are important in this regard. Investors use information from such reporting to identify how human rights issues may affect tech giants' performance, risk, and prospects, and to assess whether they are taking relevant steps to develop a long-term business strategy addressing their role and responsibilities in relation to human rights.

Integrate human rights considerations into business strategy, policy and planning

- Tech giants should make a commitment and define a strategy and adopt policies regarding respect for human rights in line with the UNGPs and other standards identified in this document.
- Tech giant policies should include measures to identify and assess actual or potential adverse human rights impacts, integrate the findings to prevent or mitigate such impacts, track effectiveness and communicate externally.
- Tech giant policies should provide for the remediation of adverse human rights impacts.
- Tech giants should regularly consider whether their remuneration, incentive systems, and wider company culture integrate respect for human rights adequately. Employees and contractors must be made aware of company strategy and policies.

Integrate human rights into risk management

- Tech giants should conduct ongoing human rights due diligence, based on the perspective of those who may be negatively impacted. They should strive to identify actual and potential negative impact on relevant human rights in relation to all aspects of a business operations. Consequently, tech giants should:
 - Identify and assess risks they pose to human rights in their activities and business models.
 - Specify actions to address identified risks, including through cessation, prevention and mitigation of potential abuses.
 - Define qualitative and quantitative indicators that enable monitoring and tracking of human rights impacts abuses caused by or otherwise linked to their activities. The performance of preventive and corrective actions should be tracked.
 - Communicate with external stakeholders including investors to account for how they address their human rights impacts.

Disclose strategy and report on human rights

- Tech giants should publicly disclose their human rights commitment, strategy, policies and processes.
- Tech giants should, for example, disclose action plans, governance structures, operational procedures and risk and impact assessments, as well as stakeholder relations with regards to human rights.
- Tech giants should ensure that information is communicated in a relevant and accessible manner.
- Tech giants should identify, monitor and at an appropriate level of detail report status of relevant human rights topics. Performance reporting should, as appropriate, use metrics that enable year-on-year comparison, in line with applicable internationally accepted reporting standards or initiatives.
- Tech giants should disclose information, at an appropriate level of detail, on activities in high-risk sectors and geographical areas and, as far as possible, be open about dilemmas they face.

Interaction with stakeholders, policy makers and regulators

- Tech giants should have policies for engaging constructively with policy-makers and regulators on human rights and be transparent about those policies or guidelines.
- Tech giants should outline their position on specific regulations relevant to their business profitability and outlook and consider promotion of policies supportive of human rights.
- Tech giants should engage with human rights bodies, governments and regulatory bodies, industry peers, and other stakeholders on human rights issues, particularly those affected by their business, products and services. This applies both in collecting the necessary information and research, as well as in building preventive and corrective action plans.
- Tech giants should establish or participate in effective and accessible operational level grievance mechanisms for negative impacts on human rights, to secure effective access to remedy for those rights-holders affected or potentially impacted by their business activities.

Context for the expectations

1. Purpose, outline and scope

This context document aims to support investors to assess and engage tech giants in fulfilling the investor expectations described above. Section 2 outlines the universal human rights standards that provide the basis of human rights expectations for states, businesses and investors, as well as tech-specific laws and guidance that protect human rights. Section 3 highlights human rights risks and impacts of special relevance to tech giants, in particular: privacy and data protection; freedom of opinion, thought and expression; elections, public and political discourse; and discrimination and at-risk groups.

This document focuses on selected human rights risks relevant to tech giants and their platforms *as such*. It does not focus on human rights risks applicable to businesses generally, for example, those linked to terms and conditions of employment amongst direct workforce or in the supply chain, or environmental sustainability issues that are addressed by existing tools and guidance.¹

Box 1. Defining tech giants and platforms

What is a “tech giant”? “Tech giants” refers to technology companies that have a dominant position in markets for internet-based platforms and services. Alphabet (Google), Amazon, Apple, Facebook and Microsoft are usually referred to as tech giants. These companies offer services and platforms linked to marketplaces, search engines, social media, application distribution platforms, payment systems and digital commerce generally. This briefing uses the term “tech giants” to refer to technology companies whose business activities, size and market position raise human rights issues that are qualitatively different to those of other businesses.²

What is a platform? “Platform” refers to a widespread services and revenue model amongst technology companies. Many tech companies operate platforms, using these to provide a wide range of consumer and other services (e.g. Uber, Airbnb). Platform business models are generally based on the collection, analysis and commercial exploitation of personal data, preferences and behaviour, which companies gather by facilitating communication and services between individuals. This data may also be exchanged with states, for example, in the context of policing and intelligence activities.³ When using platforms, individuals’ communication and behaviour is conditioned by code and companies’ policies. The dominant platforms for information search, social networking and public discourse are operated by tech giants.

Box 2. International human rights standards

Internationally-recognised human rights are set out in the [Universal Declaration of Human Rights](#) and the two primary international law instruments through which it has been codified, the [International Covenant on Civil and Political Rights](#) and the [International Covenant on Economic, Social and Cultural Rights](#) comprise the International Bill of Human Rights.

Further human rights are recognised in UN treaties on [racial discrimination](#), [discrimination against women](#), [torture and other cruel, inhuman or degrading treatment or punishment](#), [enforced disappearances](#), the [rights of children](#), [persons with disabilities](#) and [migrant workers](#). Each instrument is supervised by an independent expert body to monitor states’ compliance with treaty obligations. Additional UN instruments elaborate on the rights of groups including [indigenous peoples](#) and [national, ethnic religious and linguistic minorities](#).

Rights protected under the International Labour Organization’s (ILO) eight core conventions, set out in the [Declaration on Fundamental Principles and Rights at Work](#), are also recognized as human rights and as binding on all members of the ILO.

UN Human Rights Council and Special Procedures

The UN Human Rights Council is a body of 47 states which is responsible for the promotion and protection of human rights within the UN system. The Council's special procedures are independent human rights experts with mandates to report and advise on human rights from a thematic or country-specific perspective. Relevant special procedures in the tech giants context include the [UN Special Rapporteur on the right to privacy](#) and the [UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression](#).

Regional human rights standards

The Council of Europe's core human rights documents are the European Convention on Human Rights and the European Social Charter.⁴ The Charter of Fundamental Rights of the European Union additionally applies to EU member states⁵ along with specific protections under EU laws on equal treatment, fundamental labour and social rights and data protection, for example. EU member states' individual and shared constitutional traditions also establish baseline human rights protections within the region.

2. Business and human rights standards

2.1. Human rights: the corporate responsibility to respect and due diligence

Box 3. Business and human rights standards

The 2011 [UN Guiding Principles on Business and Human Rights](#) (UNGPs) are an authoritative global framework on business and human rights. Taking international human rights law as their baseline, the UNGPs are built on a three-pillar framework of the state duty to protect human rights, the corporate responsibility to respect human rights and victims' right to access remedy for business-related human rights abuses. The European Commission has published an [ICT sector guide on implementing the UNGPs](#).

The [OECD Guidelines for Multinational Enterprises](#) set out standards for responsible business conduct. In 2011, the OECD Guidelines were updated to include a chapter on human rights which aligns with the UNGPs. The [OECD Due Diligence Guidance for Responsible Business Conduct](#) provides practical guidance for companies on how to perform due diligence.

The UN Framework and UNGPs clarify that all businesses have a responsibility to respect internationally-recognised human rights, regardless of their size, sector, ownership or country of operation. This responsibility applies independently of whether governments in companies' home or host states fulfil their own duties to protect human rights against business-related abuses.⁶

Companies' operations can impact on the human rights of their employees, contract workers, workers in supply chains, people in communities and the environment around their operations. The human rights of individuals using companies' products or services may also be impacted. The UNGPs highlight that the corporate responsibility to respect human rights extends to a company's relationships with business partners, its value chain and other State or non-State entities directly linked to its business operations, products or services.⁷

The UNGPs highlight that businesses should, at a minimum, respect the human rights expressed in the International Bill of Human Rights⁸ and the ILO core labour standards which relate to forced labour, child labour, freedom of association and collective bargaining, and discrimination (see Box 2). Businesses are expected to adhere to additional human rights standards relevant in their circumstances. Accordingly, companies should:

- Adopt a publicly-available policy commitment to respect human rights

- Implement a human rights due diligence process to identify, assess and address their negative human rights risks and impacts, track the effectiveness of measures taken, and communicate publicly in appropriately accessible and transparent formats about their effectiveness, and
- Facilitate access to remedy for victims of human rights abuses in which they are implicated.⁹

Companies may cause, contribute or be directly linked to actual or potential human rights harm (see Box 4).

Box 4. Cause, contribution and direct linkage

According to the [UNGPs](#) and OECD Guidelines for MNEs, businesses – and investors - can be connected to human rights abuses in different ways. A business may *cause* an adverse human rights impact directly through its own acts or omissions. It may *contribute* to such an impact alongside or through other entities, including suppliers, users or customers. Finally, businesses can be *directly linked* to human rights abuses, for example through a business relationship. There is a [continuum](#) between contribution and direct linkage, which depends on the specific context and facts of the case at hand.

A company's responsibility to remediate human rights abuses with which it is involved depends on whether it caused, contributed or was directly linked to the impact concerned. The responsibility to remediate may require that a business cease conduct causing abuses, remediate abuses that have occurred, and/or use leverage over entities causing harm with which it has a business relationship.

Leverage refers to the ability to effect change in the wrongful practices of another party that is causing or contributing to an adverse human rights impact.¹⁰

2.2. Tech-specific laws and guidance

2.2.1. Government regulation

National and other governmental laws, policies and guidance including those on the internet and associated technologies, products and services regulate the role, conduct and responsibilities of technology companies. Although regulations, such as those on universal service, data protection, cybercrime, platform liability, online racism and xenophobia and child sexual abuse may not explicitly refer to human rights, they frequently have the purpose and function of protecting individuals' human rights. Examples of relevant regulations at EU level include the General Data Protection Regulation,¹¹ Directive on combating sexual abuse and exploitation of children¹² and European Digital Services Act.¹³

Recently, some states have enacted laws requiring or encouraging companies to undertake human rights due diligence as indicated by the UNGPs, while other governments and the EU have indicated the intention to do so.¹⁴ The EU Non-Financial Reporting Directive¹⁵ requires companies to publish information on their human rights policy and due diligence processes, and their supply chains, to the extent necessary for understanding their development, performance and position and impact on human rights.¹⁶ Some states have enacted requirements that companies report on data ethics in this context.¹⁷ Wherever applicable and in line with the corporate responsibility to respect human rights, tech giants should observe and implement all such rules and guidance.

2.2.2. Human rights bodies

The UN General Assembly, UN Human Rights Council, and UN special procedures have published resolutions, decisions and reports on the human rights implications of the internet and associated technologies and business practices. These have addressed, for instance, censorship via filters and the blocking of content, digital platforms, the use of algorithms and artificial intelligence.¹⁸

Likewise, the Council of Europe (COE) has developed standards on emerging threats to human rights in the digital environment. It has adopted a Convention on Cybercrime¹⁹ and guidance on online freedom of expression, internet filters, search engines, social media platforms, internet users' rights,²⁰ privacy and data

protection.²¹ The COE Recommendation on the roles and responsibilities of internet intermediaries aligns with the UNGPs and elaborates on corporate human rights responsibilities in the areas of transparency, content moderation, use of personal data and access to effective remedy.²² A further COE Recommendation considers business responsibilities linked to human rights impacts of algorithmic systems.²³ The adoption of a legal framework on human rights issues linked to the development, design and application of AI is under consideration.²⁴ Stakeholders and experts have established additional guidance and initiatives on tech companies and human rights developed as highlighted in Box 5 below.

Box 5. Tech and human rights: further guidance and stakeholder initiatives

The [Charter of Human Rights and Principles for the Internet](#) describes how universal human rights standards apply in the context of the internet and associated technologies.

The [Necessary and Proportionate Principles](#) describe how human rights should be respected in the context of surveillance of communications. The [Santa Clara Principles on Content Moderation](#) define minimum standards of transparency and accountability and call for companies to publish statistics, provide notice where content is removed and provide appeal mechanisms.

The [Manila Principles on Intermediary Liability](#) propose a human rights-based approach to legal rules defining the liability of internet intermediaries.

The Global Network Initiative (GNI) has developed a set of [voluntary principles](#) for tech and other companies addressing freedom of expression and privacy. The [Christchurch Call](#) is a commitment by governments and tech companies to eliminate terrorist and violent extremist content online which is implemented by the industry-led [Global Internet Forum to Counter Terrorism](#) (GIFCT).

[Ranking Digital Rights](#) assesses the disclosed commitments, policies and practices of internet, mobile, and telecommunications companies that affect freedom of expression and privacy of internet users and publishes an annual corporate Accountability Index.

The UN Office of the High Commissioner for Human Rights' [B-Tech project](#) aims to provide guidance on implementation of the UNGPs in the tech sector. The Danish Institute for Human Rights has produced guidance on [human rights impact assessment](#) for technology companies and on [addressing digital technologies in national action plans](#) on business and human rights.

3. Tech giants: Selected human rights risks

3.1. Human rights to privacy and data protection

The right to protection with respect to the processing of personal data forms part of the human right to respect for private and family life, home and correspondence.²⁵ Privacy is an enabling right, meaning that it secures the enjoyment of other rights, including freedom of expression.²⁶ It is strongly linked to human dignity and the free development of personality.²⁷

HUMAN RIGHTS ENGAGED

- **Privacy:** UDHR Article 12; ICCPR Article 17; ECHR Article 8; CFR (EU) Articles 7
- **Data protection:** CFR (EU) Article 8, Article 16 of the Treaty of the Functioning of the EU

3.1.1. Tech giants' collection, processing and use of personal data

Tech giants' business models assume the mass collection, processing and commercial exploitation of individuals' personal information. This includes data disclosed by individuals, and data derived by tech giants from individuals' decisions, actions and preferences in the context of internet search and social network activity and the use of other platforms and services, such as voice assistants.²⁸ Data harvested by tech giants is used to profile individuals, to predict and influence their behaviour and to target them for commercial and political purposes.²⁹

The collection of personal data interferes with the right to privacy. Detailed individual profiles may, for example, include information on sexual or political preferences derived from online behaviour. Tech giants' collection, processing and use of data are not transparent. Individuals using platforms typically have no or little effective control over what information is gathered about them or whether it is passed on to third parties. Tech giants' business model has been referred to as 'surveillance capitalism' and its compatibility with human rights questioned.³⁰

Box 6. Data protection principles under the EU General Data Protection Regulation

The EU's General Data Protection Regulation (GDPR) protects the human rights to privacy and data protection.³¹ Its requirements apply to all processing of personal data. They include data minimisation, purpose limitation, informed consent and access to data.³² The EU GDPR's concept of "data protection by design" requires a proactive approach to data protection and respecting individuals' human right to privacy from the earliest stages of product development.³³ Under privacy by design, no action may be required by an individual user to protect privacy: the highest standards must be applied by default.

- **Data minimisation:** The type and volume of personal data must be relevant and limited to what is necessary given the specific purpose of its collection. Companies must not collect more personal data than necessary or without a specific purpose.
- **Purpose limitation:** Personal data should only be collected for specified, explicit and legitimate purposes; data may not be processed in a manner incompatible with the original purpose.
- **Individual right of access to data:** Individuals must be able to access their own data collected by companies. Individuals have a right to know which personal data is being processed and with whom data is shared.
- **Consent:** An individual's consent should be a freely given, specific and informed indication of his or her agreement to the processing of the personal data in question.

3.1.2. Profiling and automated decisions

Tech giants use individuals' information to create user profiles based on their previous behaviour, "likes", interests and demographic data. These data are then exploited commercially, including as a basis for micro-targeted advertising.³⁴ Tech giants also make wide-ranging predictions about individuals' behaviour based on the analysis of data that they harvest from individuals about their conduct and preferences. AI systems may use data to make automated decisions regarding the individual. They may also transform data, removing it from its original context, so that individuals do not know or understand how their data are used or how to delete them.³⁵ Profiling and automated decision making have consequences for the right to privacy, to data protection and other human rights, for instance, those linked to political participation and to protection against discrimination (see Sections 3.3 and 3.4).

Box 7. Automated decisions under GDPR

The EU GDPR bans automated decisions that "significantly affect" the user under Article 22. Tech giants' marketing activities, which are often based on automated processing, are not explicitly prohibited under this ban, but depending on the "depth" of the profiling some marketing activities may fall within the scope of article 22 for example, if knowledge about individual characteristics are exploited in the marketing.¹

3.1.3. Encryption and anonymity

Encryption and anonymity can help to protect the human right to privacy in the online environment.³⁶ Anonymity, and the ability to control when one's identity is disclosed online can be important in safeguarding vulnerable or at-risk groups (see Section 3.4).³⁷ Tech giants should assess the need for encryption as part of their human rights due diligence process.³⁸ However, respect for human rights may also require tech giants to comply with legitimate government requests for decryption. For example, law enforcement bodies may lawfully require access to decryption of communications and identifying information held by tech giants in addressing criminality, threats to public security or safety.³⁹

3.1.4. Government access to platform data

Governments may request access to platforms' data on individual users going beyond their lawful authority to do so, in breach of the human right to privacy and data protection. Tech giants must therefore assess government requests for data to ensure any disclosure complies with data protection and human rights standards.⁴⁰ They should also disclose their policies, processes and practices in this area.⁴¹

3.2. Human right to freedom of expression

The human right to freedom of expression underpins democracy and is essential for the protection of all other human rights and freedoms. It includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. Internet platforms and social media generally facilitate communication and access to information.⁴² Given tech giants' central role as a medium for enjoyment of freedom of expression, however, their conduct may also have negative impacts on it.

HUMAN RIGHTS ENGAGED

- **Freedom of expression:** UDHR & ICCPR Article 19; ECHR Article 10; CFR (EU) Article 11

3.2.1. Internet access

Lack of access to the internet and its content can impact negatively on human rights and may reinforce existing structures of inequality, for example related to gender or to disability.⁴³ Lack of internet access is linked to denials of economic, social and cultural rights, such as the right to education, the right to an adequate standard of living and the right to health.⁴⁴ Consequently tech giants should avoid creating 'walled gardens' and promote open internet access including and beyond sectors under their control.⁴⁵

3.2.2. Internet shutdowns

Internet shutdowns deliberately prevent or disrupt access to, or dissemination of, information online. Shutdowns may be network-wide or platform-specific. They may be ordered by governments, for example, in the context of civil unrest, but executed by network operators.⁴⁶ Intentional prevention or disruption of access to information online typically violates international human rights law.⁴⁷ Tech giants may have substantial leverage with state bodies requesting or ordering shutdowns and should seek to use such leverage to avoid the abuse of human rights, in line with the UNGPs.⁴⁸

3.2.3. Illegal content

Freedom of expression is not an absolute human right: it may be legitimately restricted by states under certain circumstances.⁴⁹ Publication of some types of online content may be prohibited consistently with human rights.⁵⁰ Indeed, governments are obliged to secure the removal of content that breaches human rights. As a result, states can legitimately require tech giants and other internet intermediaries to remove various types of illegal content, for instance, via general notice-and-action obligations or through specific requests.⁵¹ Tech giants should comply with such requests in line with their corporate responsibility to respect human rights. On the other hand, tech giants have a responsibility to remove content that breaches human rights even where government does not require this.⁵²

However, the control of online content by tech giants also entails human rights risks. In general, they are poorly positioned to make the needed assessments regarding the balancing of freedom of expression with other rights and interests.⁵³ For example, tech giants may be inclined to remove too much content in order to avoid potential liability. States should thus avoid delegating responsibility to companies to adjudicate online content⁵⁴ and at minimum supervise its removal.⁵⁵

3.2.4. Legal content and “community standards”

Content moderation refers to the management by platforms of user-generated material. Through this process, tech giants remove large amounts of content held to be in violation of their “community standards”. Typically, such “community standards”, and tech giants’ internal processes applying them are not fully aligned with international human rights standards.⁵⁶ Tech giants should, by contrast, demonstrate that their terms of service, community standards and other policies governing the use of their platforms are based on and consistent with human rights standards.⁵⁷ Tech giants’ moderation policies and practices should be aligned to human rights and provide due process in relation to decisions potentially breaching human rights, for instance, decisions blocking individual or group access to platforms or regarding content removal.

3.2.5. Automated content filters

Automated content filters are deployed by tech giants to identify and remove text or images from the web or prevent their upload. Such filters are typically applied to target illegal content.⁵⁸ They operate via algorithms that analyse large volumes of data, ascertain patterns, and continually ‘learn’ from their decisions. Such filters may operate with subsequent human review or without human input. Automated content filters can prevent content previously deemed illegal from being re-uploaded to a platform.

However, automated content filters also pose risks to human rights. If they are under-sensitive, content that is illegal or in breach of human rights will not be removed. If they are over-sensitive, legal content may be removed, unduly restricting freedom of expression. Over time, as filters “learn”, they may remove additional content beyond their initially intended targets. Their algorithms may embody false and discriminatory assumptions about individuals. As filters’ ‘decisions’ are made in secret, the reasons for content removal based on them are not known to individuals, making removals hard or impossible to assess and challenge, and jeopardising due process. Accordingly, tech giants must establish human rights-aligned principles and process to ensure proportionality of any interference with human rights and adequate scope for challenges and remediation linked to removal decisions.

3.2.6. Automated content selection

When individuals search the internet using tech giants’ platforms and search engines, algorithmic decisions determine what online content they see. This can restrict the individual’s right to freedom of information. It may also contribute to fragmentation of the public sphere and polarisation of public and political debate via the creation of ‘echo chambers’

Tech giants’ platforms should adopt measures that make it possible for users to access a diversity of political views and perspectives. They should also be transparent about the use and practical impact of any automated tools they use, including the extent to which such tools deploy data harvesting, targeted advertising, and the sharing, ranking or removal of content, especially election-related content⁵⁹ (see Section 3.3 Elections, public and political discourse).

3.2.7. Terrorism and violent extremism

The UN Security Council has noted with concern the use of the internet for terrorist purposes.⁶⁰ Content arising from or intended to promote terrorism or violent extremism is addressed by specific guidelines, including the Christchurch Call⁶¹ facilitated by the Global Internet Forum to Counter Terrorism (GIFCT).⁶² On the one hand, states and companies are obliged to prevent the use of platforms for terrorist purposes to protect human rights. On the other hand, the blocking, filtering or removal of content for this legitimate

purpose can also interfere with freedom of expression if legality, proportionality or other criteria are not met.⁶³ Tech giants must therefore establish clear and human rights-aligned policies and practices in this area.

3.3. Elections, public and political discourse

HUMAN RIGHTS ENGAGED

- **Free and fair elections:** Article 21 UDHR; Article 25 ICCPR; Articles 39, 40, 41 CFR (EU).
- **Freedom of expression:** Article 19 UDHR; Article 19 ICCPR; Article 10 ECHR.
- **Privacy:** Article 12 UDHR; Article 17 ICCPR; Article 8 ECHR; Articles 7, 8 CFR (EU);
- **Life, liberty and security:** Article 3 UDHR; Articles 6, 9, 20 ICCPR; Article 6 CFR (EU)
- **Freedom from discrimination:** Article 2,7 UDHR; Articles 2, 3, 26 ICCPR; Article 14 ECHR; CEDAW; CERD.

As a principal medium for the exchange of information, including news, social and political communications, tech giants' platforms have a central function in the context of elections, public and political discourse, presenting a range of human rights risks and challenges.

3.3.1. Disinformation

Box 8. Disinformation, Mis-information and Mal-information

- **Disinformation** is “false, inaccurate or misleading information designed, presented and promoted to intentionally cause public harm or for profit”⁶⁴
- **Mis-information** describes situations where false information is shared, but no harm is meant
- **Mal-information** describes situations where genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere⁶⁵

Disinformation can distort electoral outcomes by misleading individuals or generally undermining trust in public debate and institutions, with negative consequences for the human right to free and fair elections, amongst others.⁶⁶ On the other hand, the human right to freedom of expression is not limited to ‘correct’ statements⁶⁷ so that removing disinformation from platforms can also interfere with freedom of expression in certain circumstances.⁶⁸

Accordingly, tech giants should have clear and accessible policies on disinformation that are aligned with human rights.⁶⁹ Content moderation based on such policies should be supported by appropriate due process, encompassing a right of appeal, and should apply to automated processes.⁷⁰ In addition, platforms should apply reasonable effort to address disinformation, misinformation, mal-information and election-related spam, including through independent fact-checking and other measures, such as advertisement archives, appropriate content moderation and public alerts.⁷¹

3.3.2. Political advertising and user profiling

Tech giants' platforms permit micro-targeted advertising based on individual behaviour and preferences. In political advertising, micro-targeting can be used to deliver specific messages based on targeted information intended to influence individuals' voting or other political behaviour.⁷² Such messages may contain disinformation, while their impact on the right to free and fair elections are not yet fully understood.⁷³

3.3.3. Conflict-affected areas and non-democratic states

The use of tech giants' platforms systematically to surveil individuals, targeted groups or the population at large may be linked to human rights abuses, for instance, breaches of the human rights to life, against torture or inhuman and degrading treatment, to privacy, to liberty and security of person and fair trial rights. Such risks are aggravated in conflict and post-conflict settings, as well as in countries under non-democratic rule. Human rights risks linked to disinformation may also be intensified in such settings, where in general it is difficult to verify the source and reliability of information.⁷⁴ Tech giants have the same responsibilities as other businesses under the UNGPs and should operate in conflict and post-conflict settings with heightened regard for human rights.⁷⁵

3.4. Discrimination and at-risk groups

HUMAN RIGHTS ENGAGED

- **Freedom from discrimination:** UDHR & ICCPR Article 2; ICCPR Articles 20(2), 24 and 26; ECHR Article 14; CFR (EU) Article 21; Convention on the Elimination of All forms of Discrimination Against Women (CEDAW);⁷⁶ International Convention on the Elimination of All Forms of Racial Discrimination (CERD);⁷⁷ Convention on the Rights of Persons with Disabilities (CRPD)⁷⁸
- **Gender equality:** ICCPR Article 3; CEDAW
- **Equality before the law:** UDHR Article 7 and ICCPR Article 26
- **Childrens' rights:** Convention on the Rights of the Child (CRC)⁷⁹
- **Workers' rights:** Freedom of Association and Protection of the Right to Organise Convention; Right to Organise and Collective Bargaining Convention⁸⁰

Tech giants' conduct may impact on the human right not to be discriminated against on the basis of protected characteristics, such as race, ethnicity, gender, disability, age, religion or belief or sexual orientation. Discrimination may be direct or indirect. Direct discrimination occurs when an individual is treated differently based on a protected characteristic.⁸¹ Indirect discrimination occurs where a policy or process subjects those with a protected characteristic to disadvantage.⁸² In addition, at-risk groups such as human rights defenders,⁸³ or vulnerable individuals such as those dependent on state welfare in meeting basic human needs,⁸⁴ may also be disproportionately affected by tech giants' activities in ways that harm human rights.

3.4.1. Hate speech

International human rights standards do not define "hate speech" as such.⁸⁵ However, states have a duty to protect individuals against "national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence".⁸⁶ This duty is implemented via a range of national and regional laws.

Tech giants' platforms can be used as a medium for spreading "hate speech" and for communications that seek to incite discrimination or violence.⁸⁷ Consequently human rights bodies have developed standards addressing online hate speech. The COE Convention on Cybercrime and its Additional Protocol govern hate speech motivated by racism and xenophobia.⁸⁸ The EU's Code of Conduct on Countering Illegal Hate Speech Online is a voluntary agreement subscribed to by companies including Facebook, Instagram, Microsoft and YouTube.⁸⁹ States have also enacted laws to prohibit and punish online hate speech.⁹⁰ Such legislation must be carefully applied to ensure that, while achieving its primary aim, it does not unduly restrict legitimate expression. Likewise, tech giants' content moderation policies and practices must be aligned with human rights and applied to secure these twin goals.⁹¹

3.4.2. Artificial intelligence

It is sometimes suggested that AI can eliminate unconscious bias and discrimination from public and private decision-making. Yet AI may embed discriminatory assumptions made by programmers or resulting from biases in underlying data used to 'train' algorithms.⁹² AI may thus reinforce, rather than redress, discrimination.⁹³ As a result, human rights bodies have issued standards and guidance on how human rights, including the right to freedom from discrimination, should be safeguarded in AI development. Data used to 'train' algorithms must be of sufficient quality and not embody underlying bias; its data, code, logic and development should be transparent; and algorithms' implications for human rights should be subject to impact assessment and independent oversight.⁹⁴

3.4.3. Impacts on vulnerable and at-risk groups

The human rights of vulnerable and at-risk groups may be severely impacted by abuses in the online environment. Particular issues are raised in relation to children, for instance, as regards sexual exploitation and abuse⁹⁵ and through potential impacts on their development.⁹⁶ As regards women, platforms may be utilised to threaten or incite gender-based violence and may discourage women's public and political participation.⁹⁷ This also applies to sexual and other minorities.⁹⁸ Human rights defenders may be targeted for serious human rights abuses by governments or private actors using or using information gleaned from tech giants' platforms.⁹⁹ Tech giants' policies and due diligence processes should adequately address such differentiated human rights risks and impacts.

Further resources

Privacy

United Nations

UNITED NATIONS GENERAL ASSEMBLY. 2019. Resolution 73/179. *The right to privacy in the digital age*. A/RES/73/179. Available [here](#).

UNITED NATIONS GENERAL ASSEMBLY. 2016. Resolution 71/199. *The right to privacy in the digital age*. A/RES/71/199. Available [here](#).

UNITED NATIONS GENERAL ASSEMBLY. 2014. Resolution 69/166. *The right to privacy in the digital age*. A/RES/69/166. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2019. Resolution 42/15. *The right to privacy in the digital age*, A/HRC/RES/42/15 (7 October 2019), available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2019. Resolution 41/11. *New and emerging technologies and human rights*. A/HRC/RES/41/11. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. Resolution 37/2. *The right to privacy in the digital age*. A/HRC/RES/37/2. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. "The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights". A/HRC/39/29. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2017. Resolution 34/7. *The right to privacy in the digital age*. A/HRC/RES/34/7. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2015. Resolution 28/16. *The right to privacy in the digital age*. A/HRC/RES/28/16. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2014. "Summary of the Human Rights Council panel discussion on the right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights". A/HRC/28/39. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2014. "The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights". A/HRC/27/37. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2009. Resolution 12/16. *Freedom of opinion and expression*. A/HRC/RES/12/16. Available [here](#).

UN Special Rapporteur on the right to privacy

UNITED NATIONS GENERAL ASSEMBLY. 2017. "Report of the Special Rapporteur on the right to privacy" [**Big data and open data**]. A/72/540. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2019. "Report of the Special Rapporteur on the right to privacy". A/HRC/40/63. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. "Report of the Special Rapporteur on the right to privacy" [**Review of mandate**]. A/HRC/37/62. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2017. "Report of the Special Rapporteur on the right to privacy" [**Government surveillance**]. A/HRC/34/60. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2016. "Report of the Special Rapporteur on the right to privacy" [**Mandate roadmap**]. A/HRC/31/64. Available [here](#).

Council of Europe

COUNCIL OF EUROPE. 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS. No. 108. Available [here](#).

European Union

EUROPEAN COUNCIL and EUROPEAN PARLIAMENT. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)* Available [here](#).

EUROPEAN COUNCIL and EUROPEAN PARLIAMENT. 2002. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Available [here](#).

EUROPEAN COMMISSION. 2017. "Proposal for a Regulation on Privacy and Electronic Communications". Available [here](#).

OECD

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. 2013. "The OECD Privacy Framework. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". Available at: <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

Other

RANKING DIGITAL RIGHTS. 2020. "2020 Indicators: Privacy" Available [here](#).

Freedom of expression

UN Special Rapporteur on the promotion and protection of freedom of opinion and expression

UNITED NATIONS GENERAL ASSEMBLY. 2019. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Online hate speech**]. A/74/486. Available [here](#).

UNITED NATIONS GENERAL ASSEMBLY. 2018. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Artificial intelligence**]. A/73/348. Available [here](#).

UNITED NATIONS GENERAL ASSEMBLY. 2016. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Contemporary challenges to freedom of expression**]. A/71/373. Available [here](#).

UNITED NATIONS GENERAL ASSEMBLY. 2011. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**The right to freedom of opinion and expression exercised through the internet**]. A/66/290. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2019. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Surveillance**]. A/HRC/41/35. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Online content regulation**]. A/HRC/38/35. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2017. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**The role of digital access providers**]. A/HRC/35/22. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2016. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Freedom of expression, states and the private sector in the digital age**]. A/HRC/32/38. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2015. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Encryption and anonymity**]. A/HRC/29/32. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2013. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [**States’ surveillance of communications**]. A/HRC/23/40. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [**Challenges of the internet to freedom of opinion and expression**]. A/HRC/17/27. Available [here](#).

SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. 2018. “Encryption and Anonymity follow-up report”. Research Paper 1/2018. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2013. Resolution 23/2. *The role of freedom of opinion and expression in women’s empowerment*. A/HRC/RES/23/2. Available [here](#).

Other

INVESTOR ALLIANCE FOR HUMAN RIGHTS. 2020. “Salient Issue Briefing: Freedom of Opinion and Expression”. Available [here](#).

RANKING DIGITAL RIGHTS. 2020. “2020 Indicators: Freedom of Expression and Information” Available [here](#).

SANTA CLARA PRINCIPLES ON CONTENT MODERATION. 2018 “The Santa Clara Principles on Transparency and Accountability in Content Moderation”. Available [here](#).

GLOBAL NETWORK INITIATIVE. 2017. “Implementation Guidelines for the Principles on Freedom Of Expression and Privacy”. Available [here](#).

Discrimination and vulnerable groups

United Nations

UNITED NATIONS GENERAL ASSEMBLY. 2019. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [**Online hate speech**]. A/74/486. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2020. “Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance” [**Racial discrimination and emerging digital technologies: a human rights analysis**]. A/HRC/44/57. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL 2019. “Report of the Special Rapporteur on extreme poverty and human rights” [**Digital welfare state**]. A/74/493. Available <https://undocs.org/A/74/493>.

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective” [**Online violence against women**]. A/HRC/38/47. Available [here](#).

UN WOMEN. 2020. “Online and ICT-facilitated violence against women and girls during COVID-19”. Available [here](#).

UNESCO. 2019. “Internet Universality ROAM-X Indicators”. Available [here](#).

Council of Europe

COUNCIL OF EUROPE. n.d. “Database of AI initiatives”. Available [here](#).

BROWN, ALEXANDER. 2020. “Models of Governance of Online Hate Speech”. Strasbourg: Council of Europe. Available [here](#).

COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS. 2019. “Unboxing Artificial Intelligence: 10 steps to protect Human Rights” Available [here](#).

COUNCIL OF EUROPE. 2018. “Protection of children against sexual exploitation and abuse: Child-friendly, multidisciplinary and interagency response inspired by the Barnahus model”. Available [here](#).

European Union

EU HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. 2020. "ALTAI: The Assessment List on Trustworthy Artificial Intelligence". Available [here](#).

EU HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. 2019. "Ethics Guidelines for Trustworthy AI" Available [here](#).

Other

INVESTOR ALLIANCE FOR HUMAN RIGHTS. 2019 "Salient Issue Briefing: Discrimination". Available [here](#).

Elections, public and political discourse

United Nations

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2019. "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association". [**Freedom of peaceful assembly and of association in the digital age**] A/HRC/41/41. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2014. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [**Freedom of opinion and expression in electoral contexts**]. A/HRC/26/30. Available [here](#)

SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. 2019. "Freedom of Expression and Elections in the Digital Age". Research Paper 1/2019. Available [here](#).

Council of Europe

COUNCIL OF EUROPE. n.d. "Information Disorder". Available [here](#).

COUNCIL OF EUROPE. n.d. "Dealing with propaganda, misinformation and fake news". Available [here](#).

European Union

EUROPEAN COMMISSION. 2020. "Tackling online disinformation" Available [here](#).

Other

INVESTOR ALLIANCE FOR HUMAN RIGHTS. 2020 "Salient Issue Briefing: Political Participation". Available [here](#).

RANKING DIGITAL RIGHTS and NEW AMERICA. 2020. "It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge". Available [here](#).

General

United Nations

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2016. Resolution 32/13. *The promotion, protection and enjoyment of human rights on the internet*. A/HRC/RES/32/13. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2014. Resolution 26/13. *The promotion, protection and enjoyment of human rights on the internet*. A/HRC/RES/26/13. Available [here](#).

UNITED NATIONS HUMAN RIGHTS COUNCIL. 2012. Resolution 20/8. *The promotion, protection and enjoyment of human rights on the internet*. A/HRC/RES/20/8. Available [here](#).

-
- ¹ This focus should not be read as carrying any implication regarding the potential significance, in terms of severity and likelihood, of such general business and human rights risks for tech giant companies. On severity, see further: UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Representative John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework.” A/HRC/17/31, Principle 14, Commentary. Available at: <https://undocs.org/A/HRC/17/31>.
- ² JØRGENSEN, RIKKE FRANK and AKHTAR, MARYA. 2020. “Tech-giganterne, ytrings-friheden og privatlivet”. [Tech-giants, freedom of speech and privacy]. Available at: <https://www.humanrights.dk/publications/tech-giants-freedom-speech-privacy> in Danish].
- ³ JØRGENSEN, RIKKE FRANK. 2019. “Introduction”. In: JØRGENSEN, RIKKE FRANK (ed.) *Human Rights in the Age of Platforms*, pp. xvii-xlv. Cambridge, MA: The MIT Press. Available at: <https://doi.org/10.7551/mitpress/11304.003.0004>.
- ⁴ COUNCIL OF EUROPE. 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms*. Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf; COUNCIL OF EUROPE. 2016 [1996]. *European Social Charter*. Available at: <https://rm.coe.int/the-european-social-charter-treaty-text/1680799c4b>.
- ⁵ EUROPEAN UNION. 2012 [2000]. *Charter of Fundamental Rights of the European Union*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.
- ⁶ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Representative John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework.” A/HRC/17/31. Available at: <https://undocs.org/A/HRC/17/31>.
- ⁷ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Representative John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework.” A/HRC/17/31. Available at: <https://undocs.org/A/HRC/17/31>.
- ⁸ UNITED NATIONS GENERAL ASSEMBLY. 1948. *Universal Declaration of Human Rights*. A/RES/217(III). Available at: [https://undocs.org/A/RES/217\(III\)](https://undocs.org/A/RES/217(III)); UNITED NATIONS GENERAL ASSEMBLY. 1966. *International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights*. A/RES/2200(XXI). Available at: [https://undocs.org/A/RES/2200\(XXI\)](https://undocs.org/A/RES/2200(XXI)).
- ⁹ The UN Office of the High Commissioner for Human Rights (OHCHR) has published an interpretative guide on the responsibility to respect human rights which further clarifies expectations of business under the UNGPs: OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. 2012. “The Corporate Responsibility to Respect Human Rights: An interpretative guide”. HR/PUB/12/02. Available at: <https://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf>
- ¹⁰ OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. 2012. “The Corporate Responsibility to Respect Human Rights: An Interpretative Guide”. HR/PUB/12/02. Available at: <https://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf>, p.7.
- ¹¹ EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
- ¹² EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. 2016. *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1574272335934&uri=CELEX:32011L0093>
- ¹³ EUROPEAN COMMISSION. 2020. “The Digital Services Act package”. Available at: <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>.
- ¹⁴ France’s *devoir de vigilance* requires companies to identify human rights risks and implement a *plan de vigilance* to address them. In 2020, the German Federal Government and European Commission also committed to enact human rights due diligence laws. *Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre* [Law no. 2017-399 of 27 march 2017 pertaining to the duty of vigilance of parent com-

panies and contracting companies]. Available at: <https://www.legifrance.gouv.fr/af-fichTexte.do?cidTexte=JORFTEXT000034290626&categorieLien=id> [in French]. FEDERAL MINISTRY FOR ECONOMIC COOPERATION AND DEVELOPMENT (GERMANY). “Der Nationale Aktionsplan Wirtschaft und Menschenrechte: Das nationale Rahmenwerk für Wirtschaft und Menschenrechte” [The National Action Plan for Business and Human Rights: The National Framework for Business and Human Rights]. Available at: http://www.bmz.de/de/zentrales_downloadarchiv/Presse/hintergrund-NAP-unternehmensbefragung.pdf [in German]. EUROPEAN COMMISSION. 2020. “Sustainable corporate governance”. Available at: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12548-Sustainable-corporate-governance>.

¹⁵ EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. 2014. *Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups. (Text with EEA relevance)*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0095>.

¹⁶ METHVEN O'BRIEN, CLAIRE and MARTIN-ORTEGA, OLGA. 2020. “EU Human Rights Due Diligence Legislation: Monitoring, Enforcement and Access to Justice for Victims”. *Human Rights Due Diligence Legislation - Options for the EU*. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/603495/EXPO_BRI\(2020\)603495_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/603495/EXPO_BRI(2020)603495_EN.pdf).

¹⁷ Lov nr. 642 af 19. maj 2020 om ændring af årsregnskabsloven. [Act no. 642 of 19 May 2020 amending the Danish Financial Statements Act] Available at: <https://www.retsinformation.dk/eli/lta/2020/741> [in Danish].

¹⁸ DANISH INSTITUTE FOR HUMAN RIGHTS. 2019. “United Nations Resolutions, Decisions, and reports on human rights and technology from selected UN bodies” Available at: https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/hrd_2019/un_docs_on_ict_and_human_rights_october2019.pdf; DANISH INSTITUTE FOR HUMAN RIGHTS. 2019. ‘UN: Human rights apply online as offline’ *Fact Sheet*. Available at: <https://www.humanrights.dk/publications/un-human-rights-apply-online-offline>; UNITED NATIONS GENERAL ASSEMBLY. 2018. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [Artificial intelligence]. A/73/348. Available at: <https://undocs.org/A/73/348>; UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [Content regulation and moderation]. A/HRC/38/35. Available at: <https://undocs.org/A/HRC/38/35>; UNITED NATIONS HUMAN RIGHTS COUNCIL. 2016. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [Freedom of expression, States and the private sector in the digital age]. A/HRC/32/38. Available at: <https://undocs.org/A/HRC/32/38>.

¹⁹ COUNCIL OF EUROPE. 2001. *Convention on Cybercrime*. ETS No. 185. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.

²⁰ COUNCIL OF EUROPE. 2014. *Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum*. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c6f85.

²¹ DANISH INSTITUTE FOR HUMAN RIGHTS. 2019. ‘Council of Europe standards on human rights and technology’. *Fact Sheet*. Available at: <https://www.humanrights.dk/publications/council-europe-standards-human-rights-technology>.

²² COUNCIL OF EUROPE. 2018. *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14.

²³ COUNCIL OF EUROPE. 2020. *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*. Available at: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

²⁴ COUNCIL OF EUROPE. 2020. *CAHAI – Ad hoc Committee on Artificial Intelligence*. Available at: <https://www.coe.int/en/web/artificial-intelligence/cahai>.

²⁵ European Union Agency for Fundamental Rights and Council of Europe. 2018. *Handbook on European data protection law 2018 edition*. Available at: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

²⁶ UNITED NATIONS GENERAL ASSEMBLY. 2017. “Report of the Special Rapporteur of the Human Rights Council on the right to privacy” A/72/540. Available at: <https://undocs.org/A/72/43103>, para 75.

-
- ²⁷ UNITED NATIONS GENERAL ASSEMBLY. 2017. "Report of the Special Rapporteur of the Human Rights Council on the right to privacy" A/72/540. Available at: <https://undocs.org/A/72/43103>. See further: DANISH INSTITUTE FOR HUMAN RIGHTS. 2018. "Retten til privatliv og databeskyttelse" [The right to privacy and data protection]. Available at: <https://menneskeret.dk/udgivelser/retten-privatliv-databeskyttelse> [in Danish].
- ²⁸ Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89.
- ²⁹ JØRGENSEN, RIKKE FRANK and AKHTAR, MARYA. 2020. "Tech-giganterne, ytrings-friheden og privatlivet". [Tech-giants, freedom of speech and privacy]. Copenhagen: The Danish Institute for Human Rights. Available at: <https://www.humanrights.dk/publications/tech-giants-freedom-speech-privacy> [in Danish]. citing ZUBOFF, SHOSHANA. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.
- ³⁰ ZUBOFF, SHOSHANA. 2019. "'We Make Them Dance': Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights". In: JØRGENSEN, RIKKE FRANK (ed.) *Human Rights in the Age of Platforms*. Cambridge, MA: The MIT Press. Available at: <https://doi.org/10.7551/mitpress/11304.003.0006>.
- ³¹ EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.
- ³² GDPR.EU. 2020. "What is GDPR?". Available at: <https://gdpr.eu/what-is-gdpr/>; JØRGENSEN, RIKKE FRANK and AKHTAR, MARYA. 2020. "Tech-giganterne, ytrings-friheden og privatlivet". [Tech-giants, freedom of speech and privacy]. Available at: <https://www.humanrights.dk/publications/tech-giants-freedom-speech-privacy> [in Danish].
- ³³ INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS. 2010. *Resolution on Privacy by Design*. Available at: <http://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolutions-on-Privacy-by-Design.pdf>; INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO. 2011. "Privacy by Design: The 7 Foundational Principles" Available at: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundational-principles.pdf>.
- ³⁴ AMNESTY INTERNATIONAL. 2019. "Surveillance Giants: How the business model of Google and Facebook threatens human rights". Available at: <https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>.
- ³⁵ UNITED NATIONS GENERAL ASSEMBLY. 2018. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". A/73/348. Available at: <https://undocs.org/A/73/348>, para 35.
- ³⁶ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2015. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye". A/HRC/29/32. Available at: <https://undocs.org/A/HRC/29/32>.
- ³⁷ DANISH INSTITUTE FOR HUMAN RIGHTS and GLOBAL PARTNERS DIGITAL. 2020. "The Tech Sector and National Action Plans on Business and Human Rights" Available at: <https://www.humanrights.dk/publications/tech-sector-national-action-plans-business-human-rights>, p.15; UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. 2018. "Encryption and Anonymity follow-up report" *Research Paper 1/2018*. Available at: <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>.
- ³⁸ UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. 2018. "Encryption and Anonymity follow-up report" *Research Paper 1/2018*. Available at: <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>, p. 12.
- ³⁹ Klass and Others v. Germany. European Court of Human Rights. 6 September 1978, Series A no. 28. Available at: <http://hudoc.echr.coe.int/eng?i=001-57510>
- ⁴⁰ UNITED NATIONS HUMAN RIGHTS COUNCIL. "The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights" A/HRC/27/37. Available at: <https://undocs.org/A/HRC/27/37>, para 42.
- ⁴¹ RANKING DIGITAL RIGHTS. 2020. "2020 Indicators". Available at: <https://rankingdigitalrights.org/2020-indicators/>.

-
- ⁴² UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue” A/HRC/17/27. Available at: <https://undocs.org/A/HRC/17/27>, para 22.
- ⁴³ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/RES/38/7. Available at: <https://undocs.org/A/HRC/RES/38/7>.
- ⁴⁴ LARA, JUAN CARLOS. 2015. “Internet access and economic, social and cultural rights”. Association for Progressive Communications: Johannesburg. Available at: <https://www.apc.org/en/news/connecting-your-rights-internet-access-and-economic-social-and-cultural-rights>.
- ⁴⁵ ACCESS NOW. 2015. “Open Letter to Mark Zuckerberg Regarding Internet.org, Net Neutrality, Privacy, and Security”. Available at: <https://www.accessnow.org/open-letter-mark-zuckerberg-regarding-internetorg/>.
- ⁴⁶ There were 213 internet shutdowns across 33 countries in 2019. ACCESS NOW. 2020. “#KeepItOn”. Available at: <https://www.accessnow.org/keepiton/>; UNITED NATIONS HUMAN RIGHTS COUNCIL. 2017. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”. A/HRC/35/22. Available at: <https://undocs.org/A/HRC/35/22>, paras 8-16.
- ⁴⁷ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/RES/38/7. Available at: <https://undocs.org/A/HRC/RES/38/7>; UNITED NATIONS HUMAN RIGHTS COUNCIL. 2016. *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/RES/32/13. Available at: <https://undocs.org/A/HRC/RES/32/13>; UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue” A/HRC/17/27. Available at: <https://undocs.org/A/HRC/17/27>, para 30; UNITED NATIONS HUMAN RIGHTS COUNCIL. 2017. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”. A/HRC/35/22. Available at: <https://undocs.org/A/HRC/35/22>, paras 8-16; ACCESS NOW. 2020. “ending internet shutdowns to #KeepItOn”. Available at: <https://www.accessnow.org/issue/internet-shutdowns/>.
- ⁴⁸ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2017. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”. A/HRC/35/22. Available at: <https://undocs.org/A/HRC/35/22>, para 62; SHIFT. 2013. “Using Leverage in Business Relationships to Reduce Human Rights Risks”. Available at: <https://shiftproject.org/resource/using-leverage-in-business-relationships-to-reduce-human-rights-risks/>.
- ⁴⁹ To be compatible with human rights law, any interference with freedom of expression must be prescribed by law, pursue a legitimate aim and be necessary (including proportionate). See Article 19(3) *International Covenant on Civil and Political Rights* and Article 10(2) *Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)*. See further: JØRGENSEN, RIKKE FRANK and AKHTAR, MARYA. 2020. “Tech-giganterne, ytrings-friheden og privatlivet”. [Tech-giants, freedom of speech and privacy]. Available at: <https://www.humanrights.dk/publications/tech-giants-freedom-speech-privacy> [in Danish].
- ⁵⁰ Examples include “[C]hild pornography (to protect the rights of children), hate speech (to protect the rights of affected communities), defamation (to protect the rights and reputation of others against unwarranted attacks), direct and public incitement to commit genocide (to protect the rights of others), and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life)”. UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue” A/HRC/17/27. Available at: <https://undocs.org/A/HRC/17/27>, para. 25.
- ⁵¹ JØRGENSEN, RIKKE FRANK and AKHTAR, MARYA. 2020. “Tech-giganterne, ytrings-friheden og privatlivet”. [Tech-giants, freedom of speech and privacy]. Copenhagen: The Danish Institute for Human Rights. Available at: <https://www.humanrights.dk/publications/tech-giants-freedom-speech-privacy> [in Danish].
- ⁵² The commentary to UN Guiding Principle 23 states that “Although particular country and local contexts may affect the human rights risks of an enterprise’s activities and business relationships, all business enterprises have the same responsibility to respect human rights wherever they operate. Where the domestic context renders it impossible to meet this responsibility fully, business enterprises are expected to respect the principles of internationally recognized human rights to the greatest extent possible in the circumstances, and to be able to demonstrate their efforts in this regard.” UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. “Report of the Special Representative John Ruggie. Guid-

ing Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework." A/HRC/17/31. Available at: <https://undocs.org/A/HRC/17/31>, p. 21. In Myanmar, UN investigators declared that the role of social media "is significant" in the dissemination of hate speech against the Rohingya people. UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. "Report of the independent international fact-finding mission on Myanmar". A/HRC/39/64. Available at: <https://undocs.org/A/HRC/39/64>, para 74.

⁵³ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2011. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" A/HRC/17/27. Available at: <https://undocs.org/A/HRC/17/27>.

⁵⁴ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". A/HRC/38/35. Available at: <https://www.undocs.org/A/HRC/38/35>.

⁵⁵ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". A/HRC/38/35. Available at: <https://www.undocs.org/A/HRC/38/35>, p. 7.

⁵⁶ For example, the terms of service of 'app stores' allow tech giants to operate as arbiters of freedom of expression by defining what is (and is not) made available to their users.

HESTRES, LUIS E. (2013). App Neutrality: Apple's App Store and Freedom of Expression Online. *International Journal of Communication*, 7, 1265-1280; AGENCIES. 2019. "Hong Kong protests: bring back app or risk 'complicity' in repression, Apple told" *The Guardian*. Available at: <https://www.theguardian.com/world/2019/oct/19/hong-kong-us-lawmakers-urge-tim-cook-to-restore-app-protesters-used-to-track-police>.

See also: JØRGENSEN, RIKKE FRANK, "Rights Talk: In the Kingdom of Online Giants", in *Human Rights in the Age of Platforms*, MIT Press, 2019, pp. 163-187; JØRGENSEN, RIKKE FRANK, "What platforms mean when they talk about human rights", *Internet Policy*, Vol. 9, issue 3, 2017, pp. 280-296.

⁵⁷ UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". A/HRC/38/35. Available at: <https://www.undocs.org/A/HRC/38/35>.

⁵⁸ DANISH INSTITUTE FOR HUMAN RIGHTS. 2019. Når digitale platforme skal begrænse ytringsfriheden [When digital platforms must restrict freedom of expression.] Available at: <https://menneskeret.dk/udgivelser/naar-digitale-platforme-begraense-ytringsfriheden> [in Danish].

⁵⁹ UNITED NATIONS HUMAN RIGHTS, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE and ORGANIZATION OF AMERICAN STATES. 2020. *Joint Declaration on Freedom of Expression and Elections in the Digital Age*. Available at: <https://www.article19.org/wp-content/uploads/2020/04/Joint-Declaration-Final.pdf>.

⁶⁰ UNITED NATIONS SECURITY COUNCIL. *Resolution 2396 (2017)*. Available at: [https://undocs.org/S/RES/2396\(2017\)](https://undocs.org/S/RES/2396(2017)).

⁶¹ CHRISTCHURCH CALL. 2019. *Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online*. Available at: <https://christchurchcall.com>

⁶² GLOBAL INTERNET FORUM TO COUNTER TERRORISM. 2020. Available at: <https://gifct.org>.

⁶³ UNITED NATIONS HUMAN RIGHTS COUNCIL. "Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism" A/HRC/40/52. Available at: <https://undocs.org/A/HRC/40/52>, paras 25-27.

⁶⁴ EUROPEAN COMMISSION. 2018. "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation". Available at: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>, p. 3.

⁶⁵ COUNCIL OF EUROPE. 2017. INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making. Council of Europe report DGI(2017)09. Available at: <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>.

⁶⁶ EUROPEAN COMMISSION. 2018. "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation". Available at: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>, p. 12.

-
- ⁶⁷ UNITED NATIONS HUMAN RIGHTS, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE and ORGANIZATION OF AMERICAN STATES. 2020. *Joint Declaration on Freedom of Expression and Elections in the Digital Age*. Available at: <https://www.article19.org/wp-content/uploads/2020/04/Joint-Declaration-Final.pdf>.
- ⁶⁸ UNITED NATIONS HUMAN RIGHTS, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, ORGANIZATION OF AMERICAN STATES and AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS. 2017. *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*. Available at: <https://www.osce.org/files/f/documents/6/8/302796.pdf>.
- ⁶⁹ UNITED NATIONS HUMAN RIGHTS, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, ORGANIZATION OF AMERICAN STATES and AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS. 2017. *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*. Available at: <https://www.osce.org/files/f/documents/6/8/302796.pdf>, 4a, 4b.
- ⁷⁰ UNITED NATIONS HUMAN RIGHTS, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, ORGANIZATION OF AMERICAN STATES and AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS. 2017. *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*. Available at: <https://www.osce.org/files/f/documents/6/8/302796.pdf>, 4c, 4d.
- ⁷¹ UNITED NATIONS HUMAN RIGHTS, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE and ORGANIZATION OF AMERICAN STATES. 2020. *Joint Declaration on Freedom of Expression and Elections in the Digital Age*. Available at: <https://www.article19.org/wp-content/uploads/2020/04/Joint-Declaration-Final.pdf>.
- ⁷² UNITED NATIONS HUMAN RIGHTS, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE and ORGANIZATION OF AMERICAN STATES. 2020. *Joint Declaration on Freedom of Expression and Elections in the Digital Age*. Available at: <https://www.article19.org/wp-content/uploads/2020/04/Joint-Declaration-Final.pdf>.
- ⁷³ EUROPEAN COMMISSION. 2018. "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation". Available at: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>, p. 12.
- ⁷⁴ Martin, D. A., Shapiro, J. N., & Nedashkovskaya, M. (2019). Recent trends in online foreign influence efforts. *Journal of Information Warfare*, 18(3), 15-48.
- ⁷⁵ UNITED NATIONS GENERAL ASSEMBLY. 2020. *Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises*. [Business, human rights and conflict-affected regions: towards heightened action]. A/75/212. Available at: <http://undocs.org/A/75/212>.
- ⁷⁶ UNITED NATIONS. 1979. *Convention on the Elimination of All Forms of Discrimination Against Women*. A/RES/34/180. Available at: <https://undocs.org/A/RES/34/180>.
- ⁷⁷ UNITED NATIONS. 1965. *International Convention on the Elimination of All Forms of Racial Discrimination*. A/RES/2106(XX). Available at [https://undocs.org/A/RES/2106\(XX\)](https://undocs.org/A/RES/2106(XX)).
- ⁷⁸ UNITED NATIONS. 2006. *Convention on the Rights of Persons with Disabilities*. A/RES/61/106. Available at: <https://undocs.org/A/RES/61/106>
- ⁷⁹ UNITED NATIONS. 1989. *Convention on the Rights of the Child*. A/RES/44/25. Available at: <https://undocs.org/A/RES/44/25>.
- ⁸⁰ INTERNATIONAL LABOUR ORGANISATION. 1948. *Freedom of Association and Protection of the Right to Organise Convention*. No. 87. Available at: https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO:12100:P12100_INSTRUMENT_ID:312232:NO; INTERNATIONAL LABOUR ORGANISATION. 1949. *Right to Organise and Collective Bargaining Convention*. No. 98. Available at: https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312243.
- ⁸¹ AUSTRALIAN HUMAN RIGHTS COMMISSION. n.d. "Quick Guide: Direct Discrimination". Available at: <https://humanrights.gov.au/quick-guide/12026>.
- ⁸² AUSTRALIAN HUMAN RIGHTS COMMISSION. n.d. "Quick Guide: Indirect Discrimination". Available at: <https://humanrights.gov.au/quick-guide/12049>.
- ⁸³ UNITED NATIONS GENERAL ASSEMBLY. "Report of the Special Rapporteur on the situation of human rights defenders" [Business and human rights defenders]. A/72/170. Available at: <https://undocs.org/A/72/170>; DANISH INSTITUTE FOR HUMAN RIGHTS. 2017. "National Action Plans on business and human rights Toolkit". Available at: <https://www.humanrights.dk/publications/national-action-plans-business-human-rights-toolkit-2017-edition>

-
- ⁸⁴ UNITED NATIONS GENERAL ASSEMBLY. “Report of the Special Rapporteur on extreme poverty and human rights”. [Digital technology, social protection and human rights]. A/74/493. Available at: <https://undocs.org/A/74/493>.
- ⁸⁵ UNITED NATIONS GENERAL ASSEMBLY. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”. A/74/486. Available at: <https://undocs.org/A/74/486>, p. 4.
- ⁸⁶ Article 20, *International Convention on Civil and Political Rights* and Article 4, *International Convention on the Elimination of All Forms of Racial Discrimination*.
- ⁸⁷ Religious minorities: UNITED NATIONS OFFICE ON GENOCIDE PROTECTION AND THE RESPONSIBILITY TO PROTECT. 2017. “Plan of Action for Religious Leaders and Actors to Prevent Incitement to Violence that Could Lead to Atrocity Crimes”. New York: United Nations. Available at: <https://www.un.org/press/en/2017/hr5365.doc.htm>; STEVENSON, ALEXANDRA. 2018. “Facebook Admits It Was Used to Incite Violence in Myanmar”. *The New York Times*. Available at: <https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html>;
- Refugees: OPAS, MATTHEW E. and MCMURRAY, DAVID A. 2015. “Under the gaze of the state: ICT use and state surveillance of Eritrean refugees in Italy”. *Refugee Survey Quarterly*, 34(4), pp.105-125.
- LGBT+ people: ARTICLE 19. 2018. “Challenging hate: Monitoring anti-LGBT “hate speech” and responses to it in Belarus, Kyrgyzstan, Moldova, Russia and Ukraine”. London: Article 19. Available at: https://www.article19.org/wp-content/uploads/2018/03/LGBT-Hate-Speech-Report-Central-Asia_March2018.pdf;
- Women: UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. “Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective”. A/HRC/38/47. Available at: <https://undocs.org/A/HRC/38/47>;
- Persons of colour: TYNES, BRENDISHA M. “Online racial discrimination: A growing problem for adolescents” *American Psychological Association Science Brief*. Available at: <https://www.apa.org/science/about/psa/2015/12/online-racial-discrimination>; UNITED NATIONS GENERAL ASSEMBLY. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”. A/74/486. Available at: <https://undocs.org/A/74/486>, para 4.
- ⁸⁸ COUNCIL OF EUROPE. 2001. *Convention on Cybercrime*. ETS No. 185. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>; COUNCIL OF EUROPE. 2003. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. ETS No. 189. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
- ⁸⁹ EUROPEAN COMMISSION. 2016. *The EU Code of conduct on countering illegal hate speech online*. Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#theeucodeofconduct.
- ⁹⁰ HADAVAS, CHLOE. 2020. “France’s New Online Hate Speech Law Is Fundamentally Flawed: What could a better approach look like?”. *Slate*. Available at: <https://slate.com/technology/2020/05/france-hate-speech-law-lutte-contre-haine-sur-internet.html>.
- ⁹¹ “However, the use of algorithms to curate social media content and encourage people to remain on the platform can result in Google and Facebook actively promoting or amplifying abusive, discriminatory or hateful content. The platforms recommend and promote new content based on opaque algorithmic processes to determine what will best engage users. Because people are more likely to click on sensationalist or incendiary material, the so-called ‘recommendation engines’ of these platforms can send their users down what some have called a ‘rabbit hole’ of toxic content.” AMNESTY INTERNATIONAL. 2019. “Surveillance Giants: How the business model of Google and Facebook threatens human rights”. Available at: <https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>, p. 34.
- ⁹² For example, Amazon’s reported AI recruitment tool which was found to discriminate against women – it’s machine learning was based on a dataset of previous applicants for positions over a 10 year period, the majority of whom were male. DASTIN, JEFFREY. 2018. “Amazon scraps secret AI recruiting tool that showed bias against women”. *Reuters*. Available at: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>.
- ⁹³ UNITED NATIONS GENERAL ASSEMBLY. 2018. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”. A/73/348. Available at: <https://undocs.org/A/73/348>; COUNCIL OF EUROPE. 2017. “Algorithms and human rights: Study on the human rights dimensions of automated data processing

techniques and possible regulatory implications”. DGI(2017)12. Strasbourg: Council of Europe. Available at: <https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10>, p.27.

⁹⁴ COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS. 2019. “Recommendation – Unboxing Artificial Intelligence: 10 steps to protect Human Rights”. Strasbourg: Council of Europe. Available at: <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>; COUNCIL OF EUROPE. 2020. *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*. Available at: https://search.coe.int/cm/pages/result_details.aspx?objectId=09000016809e1154; FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. 2018. “Big data, algorithms and discrimination”. Luxembourg: EU Publications Office. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-in-brief-big-data-algorithms-discrimination_en.pdf; EUROPEAN COMMISSION. “Ethics Guidelines for Trustworthy AI: Report of the High-Level Expert Group on Artificial Intelligence” Available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

⁹⁵ The *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* set out an approach to addressing risks for children online, but without an explicit human rights framing.

FIVE COUNTRY MINISTERIAL. 2020. *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* Available at: <https://www.justice.gov/opa/press-release/file/1256061/download>

⁹⁶ KARDEFELT-WINTHER, DANIEL. 2019. “Responding to Screen Time Concerns: A Children’s Rights Approach” UNICEF *Evidence for Action Blog*. Available at: <https://blogs.unicef.org/evidence-for-action/screen-time-concerns-children-participation-digital-online/>; COMMITTEE ON THE RIGHTS OF THE CHILD. 2020. “General Comment on children’s rights in relation to the digital environment” [Drafting process]. Available at: <https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx>

⁹⁷ **Sextortion** refers to the use of ICT to blackmail a victim. In such cases, the perpetrator threatens to release intimate pictures of the victim in order to extort additional explicit photos, videos, sexual acts or sex from the victim. **Doxing** refers to the publication of private information, such as contact details, on the Internet with malicious intent, usually with the insinuation that the victim is soliciting sex (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of exposing the woman to the “real” world for harassment and/or other purposes). It includes situations where personal information and data retrieved by a perpetrator is made public with malicious intent, clearly violating the right to privacy. **Trolling** consists in the posting of messages, the uploading of images or videos and the creation of hashtags for the purpose of annoying, provoking or inciting violence against women and girls. Many “trolls” are anonymous and use false accounts to generate hate speech. UNITED NATIONS HUMAN RIGHTS COUNCIL. 2018. “Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective”. Available at: <https://undocs.org/A/HRC/38/47>, paras 31-33; INTER-PARLIAMENTARY UNION. 2016. “Sexism, harassment and violence against women parliamentarians”. Available at: <http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf>; PENNEY, JONATHON. 2017. “Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study”. 6(2) *Internet Policy Review*, Available at: <https://ssrn.com/abstract=2959611>

⁹⁸ ARTICLE 19. 2018. “Challenging hate: Monitoring anti-LGBT “hate speech” and responses to it in Belarus, Kyrgyzstan, Moldova, Russia and Ukraine”. Available at: https://www.article19.org/wp-content/uploads/2018/03/LGBT-Hate-Speech-Report-Central-Asia_March2018.pdf

⁹⁹ OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. 2018. “The double-edged of new technology for human rights defenders”. Available at: <https://www.ohchr.org/EN/NewsEvents/Pages/HumanRightsDefenders.aspx>.