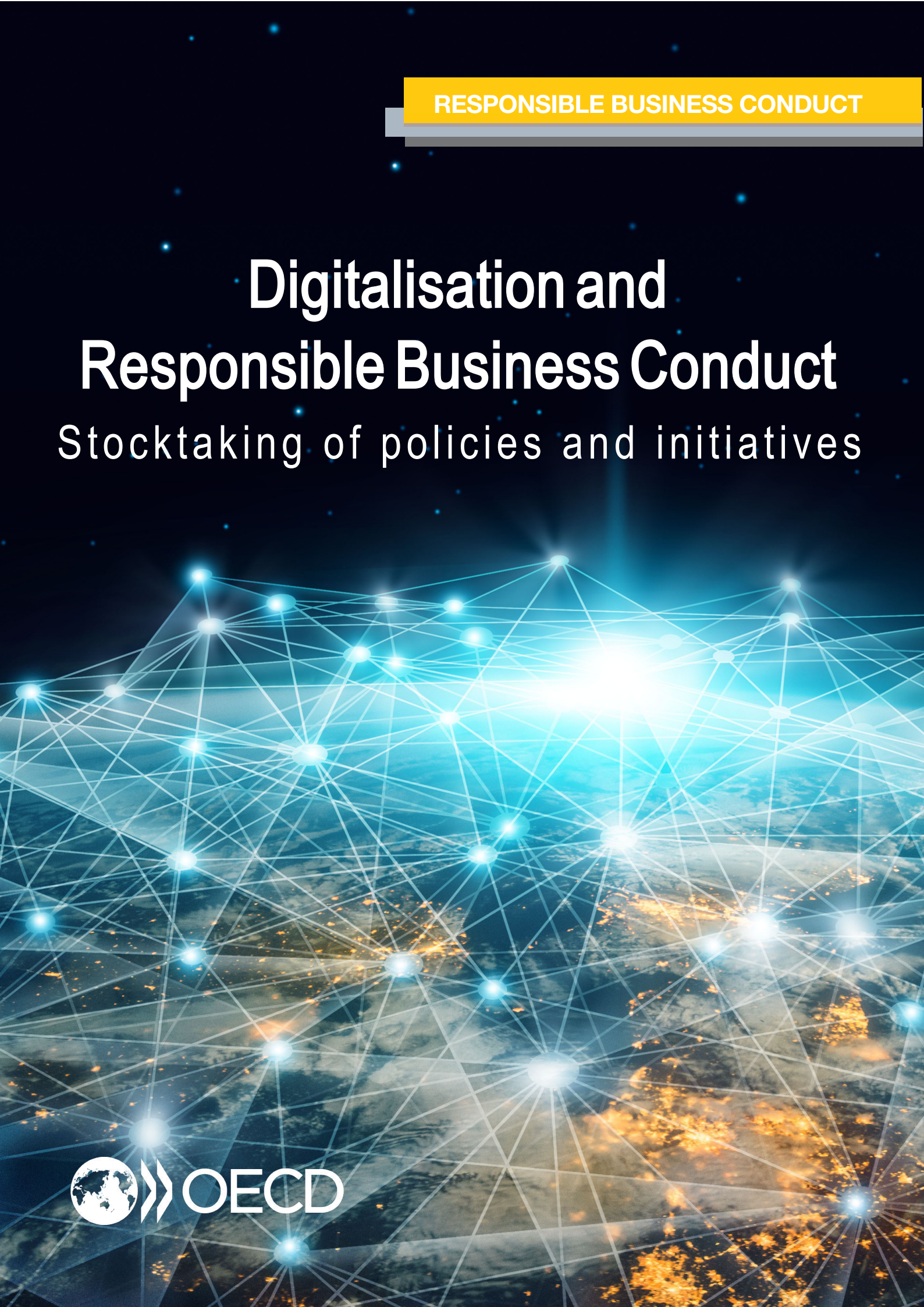
RESPONSIBLE BUSINESS CONDUCT

Digitalisation and Responsible Business Conduct

Stocktaking of policies and initiatives



OECD

Please cite this paper as:

OECD (2020), Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives

This paper has been prepared by the OECD Centre for Responsible Business Conduct, under the supervision of Tyler Gillard, Head of Due Diligence, and the overall guidance of Cristina Tébar Less, Acting Head of the Centre. The team that drafted the paper comprised Rashad Abelson and Marjoleine Hennis. Consultants from Article One Advisors supported the research and Juliet Lawal and Ariane Rota provided communications support.

This paper is part of the Centre's work on digitalisation with the financial support of the Netherlands.

Table of contents

Figures

Boxes

Executive Summary

The digital economy has had a profound impact on society, including the global business landscape and market dynamics. New phenomena such as online platforms, social media, distributed ledger technology (such as blockchain), big data and online service providers affect business models and our understanding of what a "business" is. It has changed the notion of the "multinational enterprise" with the emergence of new forms of firms and industries operating internationally, such as the platform economy, many of which were "born global" and are not linked to a specific country. Digitalisation has a significant impact on the workplace, and has driven innovation in all sectors, but has also contributed to the transformation and disruption of traditional industries.

The links between digitalisation and Responsible Business conduct (RBC) are manifold. New digital tools can help firms accelerate their contribution to sustainable development, and enable businesses to strengthen their efforts to meet standards of RBC. At the same time, digitalisation can also cause business to violate human rights, or contribute to social and environmental harms in new ways. These changes affect the specific roles and responsibilities of business and governments to promote and implement RBC standards in a digital world. Governments are confronted with new opportunities and challenges while promoting the implementation of RBC standards, including the OECD Guidelines for Multinational Enterprises in a rapidly evolving and multi-disciplinary context.

A review of international standards and initiatives on digitalisation by international organisations and governments, as well as efforts by various stakeholders shows that a majority of standards and initiatives seek to address, in some form, various RBC issues. They primarily focus on the conduct of entities involved in the development or (mis)use of digital technologies, and their impacts on science and technology, workers (including the future of work), consumers, and human rights (specifically privacy, freedom of expression, political participation, and discrimination at the workplace). Considerations related to competition and taxation also feature heavily in the initiatives, while few deal with environmental issues in depth.

RBC instruments, such as the OECD Guidelines for Multinational Enterprises, OECD due diligence guidance, and the United Nations Guiding Principles on Business and Human Rights are relevant and useful, in that they provide an overarching framework for business to categorise and frame their adverse impacts in a systematic way. However, RBC instruments are not the driving force behind new standards and initiatives that often tend to be very "issue focused" and sometimes "incident driven".

National-level Artificial Intelligence (AI) standards and initiatives largely focus on developing AI strategies, rather than regulation, and economic opportunities are driving state AI policies and research investments. The dominant focus areas in strategies dealing with AI in relation to RBC are competition issues (43%), human rights, including privacy and discrimination in the workplace (43%), labour market impacts, specifically on the future of work (41%) and consumer protection (39%). Approximately 35% of the strategies also foresee some action on disclosure of AI systems by developers or users.

In relation to online platforms, the impacts of social media have received increased attention by governments, triggering higher rates of legislation. Legislation has largely focused on content moderation, especially around terrorist activity and the spread of false information. In some cases, companies face criminal and financial penalties. A majority of social media regulation is motivated by the risk of offline harm, respecting and enforcing existing laws on online platforms. 92% also connect this issue to consumer interests, and foresee some element of disclosure around content moderation. Labour issues only come up in around 21% of the regulations reviewed. Environmental and corruption issues rarely feature.

Multi-stakeholder initiatives are playing a critical role in helping clarify specific RBC issues in relation to digital technologies, and they support common action. Civil society is actively involved in defining and promoting ethical principles for responsible development and the use of digital technologies. While not consistent, many of the emerging principles reference some international RBC instruments.

Introduction

This paper was developed by the OECD Centre for Responsible Business Conduct as part of an ongoing consideration of the links between the digitalisation of the global economy and responsible business conduct (RBC). RBC encompasses a range of issues, including human rights abuses, consumer protection, environmental degradation, taxation, and corruption among others, as described in the OECD Guidelines for Multinational Enterprises (MNE Guidelines).[1]

Given the broad scope and far reaching effects of digitalisation, the OECD Working Party on Responsible Business Conduct (WPRBC) instructed the Secretariat to take stock of initiatives by governments and international organisations, as well as civil society, multi-stakeholder and business-led efforts linking RBC with digitalisation. These efforts include, for example, national strategies, legislation, research, government and civil society recommendations, and industry-led and multi-stakeholder working groups.[2] The paper is structured as follows:

Section 1 discusses the links between RBC and digitalisation and summarises the key issues and findings emerging from the stocktaking and analysis of current initiatives described in sections 2 and 3. This section also seeks to explain the relevance of the MNE Guidelines for the development or use of digital technologies, and provides some initial general findings.

Section 2 provides a description of relevant international standards and initiatives related to digitalisation within the OECD and other international organisations, including at the regional level. The section highlights OECD instruments and efforts in the field of digital technologies which are underway or planned, and which touch upon the various areas covered by the MNE Guidelines. Given the importance of supporting coherence within the OECD on this topic, this part of the report aims to be relatively exhaustive in describing these standards and initiatives.

Section 3 contains an overview of selected national regulations, policies, instruments and initiatives by civil society, and industry. It is non-exhaustive, and does not provide the same level of detail as information contained in Section 2. Nonetheless, it seeks to capture some of the main developments in this field, and offers some preliminary analysis of those efforts in relation to RBC.

The Annex of the paper provides detailed information on all the standards and initiatives described in Section 3.

[1] OECD, Guidelines for Multinational Enterprises [http://mneguidelines.oecd.org/mneguidelines/; OECD/LEGAL/0144], referred to throughout this note as the "MNE Guidelines" or simply the "Guidelines" where it is clear that it is the MNE Guidelines being referenced.

[2] Although the development of distributed ledger technology (commonly referred to as 'blockchain') is relevant to digitalisation, this paper was limited in scope to artificial intelligence and online platforms. For more information on linkages between blockchain and RBC, see the 2019 OECD RBC Centre paper *Is there a role for blockchain in responsible supply chains?,* https://mneguidelines.oecd.org/is-there-a-role-for-blockchain-in-responsible-supply-chains.htm.

1. Linking responsible business conduct and digitalisation

Relevance of the OECD Guidelines for Multinational Enterprises for the digital economy

The digital economy has had a profound impact on society, including the global business landscape and market dynamics. New phenomena such as online platforms, social media, distributed ledger technology (such as blockchain), big data and online service providers affect business models and our understanding of what a "business" is. It has changed the notion of the "multinational enterprise" with the emergence of new forms of firms and industries operating internationally, such as the platform economy, many of which were "born global" and are not linked to a specific country. Digitalisation has a significant impact on the workplace, and has driven innovation in all sectors, but has also contributed to the transformation and disruption of traditional industries.

The OECD Guidelines for Multinational Enterprises (MNE Guidelines) are voluntary principles and standards for RBC recommended by governments to business. They acknowledge and encourage the positive contributions that business can make to economic, environmental and social development, and also recognise that business activities can result in adverse impacts related to workers, human rights, the environment, bribery, consumers and corporate governance. All the specific adverse impacts are listed out in the various chapters of the MNE Guidelines. The MNE Guidelines also represent a commitment by governments to protect the public interest and a responsibility to provide an enabling framework for RBC.

The MNE Guidelines set out the expectation for businesses to act responsibly by conducting due diligence on their operations and those of their supply chain, so that they can identify and address risks of causing, contributing, or being directly linked to negative impacts. The OECD Due Diligence Guidance for Responsible Business Conduct provides practical support to enterprises on the implementation of the OECD Guidelines for Multinational Enterprises by providing plain language explanations of its due diligence recommendations and associated provisions. Implementing these recommendations can help enterprises avoid and address adverse impacts related to workers, human rights, the environment, bribery, consumers and corporate governance that may be associated with their operations, supply chains and other business relationships. The OECD has also developed sector specific guidance for carrying out supply chain due diligence in minerals, garment and footwear, agriculture, as well as for institutional investors.

The links between digitalisation and RBC are manifold. New digital tools can help firms accelerate their contribution to sustainable development, and enable businesses to strengthen their efforts to meet standards of RBC (see Box 1). At the same time, digitalisation can cause business to violate human rights, or contribute to social and environmental harms, in new ways. These changes affect the specific roles and responsibilities of business and governments to promote and implement RBC standards in a digital world. Governments and National Contact Points are confronted with new opportunities and challenges while promoting the implementation of RBC standards, including the MNE Guidelines, in a rapidly evolving and multi-disciplinary context.

The present report intends to provide Adherents with some preliminary information to support an informed discussion about the application of the MNE Guidelines with respect to the development and use of digital technologies.

Box 1. Overview of digital technologies

Digital technologies are electronic tools, systems, devices and resources that generate, store or process data. Well-known examples of their application include social media, online games, and mobile phones. Digital technologies have considerably speeded up data transmissions, transforming the way people communicate and work.

Digitalisation is understood as the use of digital technologies and data, as well as interconnection that results in new activities, or changes to existing activities. **Digital transformation** refers to the economic and societal effects of digitisation and digitalisation.[3]

An important element of the digital transformation has been the emergence of new business models, such as online platforms. An **online platform** is "a digital service that facilitates interactions between two or more distinct, but interdependent, sets of users (whether firms or individuals) who interact through the service via the Internet, and for which generating and working with user data is an important feature that sets them apart from other businesses.[4] Online platforms include a range of services available via the internet – including for example, online marketplaces (e.g. Etsy and E-Bay), search engines (e.g. Google and Baidu), social media (e.g. Facebook and Twitter), app stores (e.g. Apple App Store), communication services (e.g. WhatsApp and WeChat), payment systems (e.g. Venmo and PayPal), and platforms supporting the gig economy (e.g. Uber and Task Rabbit), among others. Online platforms have emerged rather recently and they operate within a relatively limited regulatory framework.

Digital technologies have made **Artificial Intelligence** (AI) possible. An AI system is designed to have a machine accomplish a specific problem-solving or reasoning task. The system is based on the collection of data through sensors. With the help of these data, it produces a model of the environment, and with the help of algorithms it interprets this environment.[5] Thanks to increased storage capacity and the possibility to analyse large quantities of data (big data), AI increasingly uses machine learning (defined below).

Machine Learning (ML) is a set of techniques that allow machines to learn in an automated manner through patterns and inferences, rather than through explicit instructions from a human. This has led to a considerable increase of the potential of AI in making predictions and decisions.[6]

For an introduction to AI and online platforms, and their implications for RBC, see the notes presented at a workshop on 4 November 2019: AI - https://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf; Blockchain - https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf; Online platforms - https://mneguidelines.oecd.org/RBC-and-platform-companies.pdf.

[3] OECD (2019), Going Digital: Shaping Policies, Improving Lives, OECD Publishing, Paris, https://doi.org/10.1787/9789264312012-en, p. 18

[4] OECD (2019), An Introduction to Online Platforms and Their Role in the Digital Transformation, OECD Publishing, Paris, https://doi.org/10.1787/53e5f593-en.

[5] OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, https//doi.org/10.1787-en, p. 23

[6] OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, https//doi.org/10.1787-en, p. 27

RBC standards may be relevant for digitalisation in a number of ways. Business may use new digital technologies for its own purposes, which in turn could have new or unforeseen adverse impacts on matters covered by the MNE Guidelines. For example, companies using AI for monitoring the productivity of their employees, or for gathering data of their clients or consumers.

RBC standards may also be relevant when businesses develop a digital technology, or make it available to others, including to other business or private individual users. An example are online platforms and their responsibility vis-à-vis other users/consumers for violent content.

Finally, the use of digital technologies can improve and accelerate a business's own efforts to meet RBC standards. For example, AI, big data, and machine learning may support supply chain due diligence by more efficiently identifying, prioritising, and tracking RBC risks. Blockchain can enhance due diligence by creating higher transparency within global supply chains and by reducing fraud.

Depending on the use of the specific digital technology, the actors in the value chain may differ.[7] In considering the implications of the MNE Guidelines for the "digital value chain", it may be useful to distinguish the following actors: the developers of an application of digital technology; the vendors; those that provide the necessary infrastructure (to make the technology available to others, like data collection, internet hosts, transit providers, browsers and search engines); and the users or consumers.

Preliminary observations from stocktaking of standards and initiatives

Given the limitations on resources and time, the stocktaking is not exhaustive, and varies in the level of detail and analytical depth. As described above, whereas the stocktaking of OECD efforts seeks to be exhaustive, stocktaking of efforts by governments and stakeholders are still high-level, due to the large and diverse range of policies, standards and initiatives that are emerging in this field. Nonetheless, a number of initial, crosscutting observations may be useful.

- A vast majority of standards and initiatives on digitalisation seek to address, in some form, various RBC issues. Primarily these issues surround the conduct of entities involved in the development or (mis)use of digital technologies, and their impacts on science and technology, workers (including the future of work), consumers, and human rights (specifically privacy, freedom of expression, political participation, and discrimination at the workplace). Considerations related to competition and taxation also feature heavily in the initiatives reviewed. While the digital transformation is considered to have impacts on the environment, with its high energy consumption on the one hand, and its potential to help entities better manage environmental impacts on the other, most standards or initiatives reviewed are not dealing with these issues in depth, as they are not considered yet to be the most material challenge of the digital transformation.
- RBC instruments, such as the MNE Guidelines, OECD due diligence guidance, and the United Nations Guiding Principles on Business and Human Rights, are not driving these processes per se. For the most part, there is a notable absence of reference or use of RBC instruments in existing digitalisation policies, standards or initiatives. Digitalisation policies and standards are often dealing with very specific, and in some cases, new forms of adverse impacts that are emerging, and tend to be very "issue focused" and sometimes "incident driven".

[7] See the OECD note on AI and RBC for an overview of seven use cases or patterns, https://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf.

- At the same time, RBC instruments, including the MNE Guidelines and OECD due diligence guidance, do cover the issues dealt with by the digitalisation standards or initiatives at a general level. RBC instruments are therefore relevant and useful, in that they provide an overarching framework for business to categorise and frame their adverse impacts in a systematic way (e.g. along chapters of the Guidelines), and to undertake due diligence to identify and address risks, including those related to digitalisation. The Guidelines and OECD due diligence guidance have a proven record for enabling business to operationalise due diligence in a variety of sectors and interactions with society. RBC instruments will likely continue to be used by stakeholders as a key reference for the responsible development and use of digital technologies, and National Contact Points may see an increase in specific instances on these issues as a result.[8] However, given that RBC instruments do not yet contain the level of specificity needed to be directly used in policy and practice, further elaboration of what RBC instruments mean for governments and industry in the digital transformation could be particularly useful.

Specific observations in relation to efforts by different stakeholder groups are elaborated further below.

Observations on efforts by the OECD and other international organisations

The stocktaking in Section 2 gives an overview of OECD standards and initiatives in the field of digitalisation to the extent that they are relevant for RBC. It examines more in detail the debate about digitalisation in the OECD and in how far the use, misuse, and access to digital technologies is covered, or in line with the principles of RBC.

Section 2 includes a review of OECD legal instruments in this space, and other relevant initiatives in the OECD. In addition, it describes five standards and seven initiatives of other International Organisations in this field. These cover a wide variety of issues, ranging from the very specific and technical, such as the Recommendation on Responsible Innovation in Neurotechnology, to the more broad, such as the Privacy Guidelines.

Since the 1980s, the OECD has adopted a number of standards that refer to digital technologies. For the purposes of this report, they can be subdivided into the following groups: standards related to the (re)use, access and governance of data, such as the Privacy Guidelines; standards related to digital security, such as the Security Guidelines; standards for the use of digital technologies, such as the Recommendation on Artificial Intelligence; and standards for policy making in view of the digital transformation, such as the Recommendation of the Council on Consumer Protection in E-commerce.

Parallel to the developments in the OECD, other International Organisations have developed similar or complementary standards. For example, the UN B-tech project seeks to cover a wide range of human rights topics and enable business to implement the UN Guiding Principles on Business and Human Rights when using new digital technologies. Given the alignment between the UN Guiding Principles on Business and Human Rights and the human rights chapter of the MNE Guidelines, it will be useful to continue to engage with the UN Office of the High Commissioner for Human Rights and the Working Group on Business and Human Rights in this field.

[8] So far, the number of cases with a digital component has been rather limited, with only one specific instance brought to an NCP in 2018, and one during the first 6 months of 2020. These specific instances both involved digital platforms, respectively Grupa OLX and AirBnB. See: For an overview of specific instances see: https://mneguidelines.oecd.org/database/.

Observations on government efforts

Section 3 takes stock of government efforts on artificial intelligence (including national strategies, legislation, research and government recommendations), and on social media and online platforms (including national strategies, legislation, and recommendations).

In relation to AI, some initial observations include:

- Governments are largely focused on developing AI strategies rather than regulation. Since 2015, countries increasingly include AI strategies in their national policies. This is particularly the case in OECD countries and key partners. Regulation on artificial intelligence appears to remain minimal, with a clear concern from governments that they do not limit innovation with regulation that may place their country at a global disadvantage.
- At the same time, governments are increasingly developing strategies to advance their own efforts to create a conducive environment to innovation and digital transformation. Strategies commonly focus on the future of work, research, and incentivising innovation and leadership.
- Economic opportunities are driving state AI policies and research investments. Several states designate how AI will help specific sectors of their economies, often including agriculture, industry, healthcare and smart cities. At the same time, most national strategies or policies on AI address, in some form, the actual or potential impacts that artificial intelligence may have on people, planet and society.
- The dominant focus areas in strategies dealing with AI in relation to RBC are competition issues, human rights, including privacy and discrimination in the workplace, labour market impacts, specifically on the future of work and consumer protection. About 40% of the strategies reviewed mention one or several of these elements. In addition, approximately 35% of the strategies reviewed also foresee some action on disclosure of AI systems by developers or users.

In relation to online platforms:

- Europe is the most active region in terms of regulatory efforts. The General Data Protection Regulation (GDPR) and the UK's online safety initiative are paving the way for a more holistic approach in protecting the users of online platforms and defining online platforms' responsibilities.
- The impacts of social media have received increased attention by governments, triggering higher rates of legislation. Legislation has largely focused on content moderation, especially around terrorist activity and the spread of false information. In some cases, companies face criminal and financial penalties. A majority of social media regulation is motivated by the risk of offline harm, respecting and enforcing existing laws on online platforms.
- Civil society and some governments have raised concerns that over-regulation will result in infringements on the right to free expression. At the same time, governments and stakeholders continue to acknowledge the need to identify and prevent terrorist, violent and extremist content online. The Sharing of Abhorrent Violent Material Bill in Australia is a notable example of legislative efforts aimed at balancing these objectives.
- Government and industry collaboration is considered to be fundamental to ensuring competition in the digital economy. Particularly in this field, regulation risks lagging behind. In order to ensure "RBC by design", i.e. the integration of RBC considerations in the technology right from the beginning, governments will need to be closely engaged with the business sector and other experts. Without tech-sector and stakeholder collaboration, governments may also encounter significant pushback and fall behind in the global tech race.

- All of the regulations and standards reviewed address, in some form, human rights. 92% also connect this issue to consumer interests, and foresee some element of disclosure around content moderation. Labour issues only come up in around 21% of the regulations reviewed. Environmental and corruption issues rarely feature.

Observations on efforts of multi-stakeholder initiatives, industry, and other stakeholders

Section 3 also takes stock of numerous stakeholder standards and initiatives. In relation to multi-stakeholder efforts, the stocktaking reviews 24 multi-stakeholder initiatives and partnerships, including partnerships with International Organisations. In addition, it covers 12 civil society-led initiatives, which primarily focus on voluntary initiatives, whitepapers, civil society or academic recommendations, ratings and rankings. In order to get insight into specific company behavior, it also maps 12 company AI principles and guidelines, and 6 social media policies, including user agreements and community standards.

Some initial observations include:

- Multi-stakeholder initiatives are playing a critical role in helping clarify specific RBC issues in relation to digital technologies and support common action. For example, the *Global Network Initiative* provides a framework of principles and oversight for the ICT industry to respect, protect, and advance user rights to freedom of expression and privacy, in particular as it relates to requests for information by governments. The *Christchurch Call* outlines commitments from Governments and online service providers to address terrorist and violent extremist content online, and to prevent the abuse of the internet as occurred in and after the Christchurch attacks. The *Partnership on AI* primarily focuses on stakeholder engagement and dialogue seeking to maximise the potential benefits of AI for as many people as possible.
- Civil society is actively involved in defining and promoting ethical principles for responsible development and use of digital technologies. While not consistently, many of the emerging principles reference some international RBC instruments (mostly from the United Nations). Leading efforts include the Santa Clara Principles, which call for transparency by social media companies by publishing the numbers of removed posts, notifying users of content removal, and providing opportunities for meaningful and timely appeals. The Toronto Declaration is a human rights-based framework that delineates the responsibilities of states and private actors to prevent discrimination with AI/ML advancements. Ranking Digital Rights is the first public tool to assess company performance on digital rights, seeking to trigger a ‘race to the top’.
- Companies have developed detailed policies dealing with a wide range of RBC issues. For AI, company policies tend to focus on transparency of AI systems, promotion of human values, human control of technology, fairness and non-discrimination, safety and security, accountability, and privacy. For online platforms, company policies tend to focus on mitigating violence and criminal behaviour, safety, mitigating objectionable content, integrity and authenticity, data collection, use, and security, sharing of data with third parties, user control, accountability, and promotion of social welfare. Broad commitments to human rights are included in most company policies reviewed. A brief analysis of 12 company efforts shows that while many companies have publicly committed to human rights, their due diligence commitments largely focus on identifying and managing risk related to the above-mentioned policy issues, rather than tracking effectiveness, public reporting, or supporting remediation.

Conclusions and ways forward

Given the wide-ranging RBC issues addressed in this stocktaking review, OECD RBC instruments continue to be relevant. They can provide cross-sectoral frameworks for looking at these issues holistically, and can help connect the dots between the different RBC issues. The broad scope of the MNE Guidelines, covering all areas where business interacts with society, allows for addressing the manifold impacts of digitalisation on society and to enhance the use of new technologies for actually improving RBC and supply chain due diligence. OECD RBC instruments can also reinforce cooperation between new types of companies involved in the digital transformation and the companies in the real economy that are already familiar with RBC instruments (and who are increasingly making use of new forms of technology). Specifically, the MNE Guidelines and Due Diligence Guidance enable business to systematically address the impacts of their activities in all of their interactions with society. At the same time, it is clear from the review that policy-makers, National Contact Points for RBC (NCPs), industry, workers and other stakeholders could benefit from further work to integrate RBC standards and approaches into ongoing digitalisation efforts, and clarify the applicability of RBC instruments to specific digital issues.

2. International standards and initiatives

This section gives an overview of standards and initiatives at the OECD and other International Organisations (IOs) in the field of digitalisation to the extent that they are relevant for RBC. It specifically highlights the debate about digitalisation in the OECD and in how far the use, misuse, and access to use of digital technologies is covered or in line with RBC standards.

OECD standards related to digitalisation

Since the 1980s, the OECD has developed a number of standards that refer to digital technologies. For the purposes of this report, they can be subdivided into the following groups: standards related to the (re)use, access and governance of data; standards related to digital security; standards for the use of digital technologies; and standards for policy making in view of the digital transformation. A selection of the most important OECD standards and their links with RBC are discussed below.

(Re)use, access and governance of data

There are many different approaches to the governance of cross-border data flows, resulting from different policy objectives and cultural preferences[9]. The OECD discussion reflects this. It has centred around a search for a balance between the unlimited flow of data, freedom of expression and the need to protect individuals (for example, against violent content on the web), and/or between the right to privacy and innovation (for example, when using big data that considerably improve the diagnostics of patients).

Since the mid-1970s, the OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. In 1980, the *Recommendation* of the Council *concerning* ***Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines")*** was adopted. It constituted the first internationally agreed-upon set of privacy principles.[10] The Privacy Guidelines apply to personal data in the public or private sector which, because of their nature, the way there are processed, or the context in which they are used, pose a risk to privacy and individual liberties.

In addition to the Privacy Guidelines, references to the protection of data were included in the ***Recommendation of the Council on Cross-Border Cooperation in the Enforcement of Laws against Spam*** of 2006.[11] This Recommendation can be seen as one of the forerunners of OECD Recommendations on privacy protection and cross border data governance. It dealt with the challenges of electronic communication and cross border information gathering and sharing, such as the protection of personal information of individuals. Cross border co-operation, through the

[9] Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris. http://dx.doi.org/10.1787/b2023a47-en

[10] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188]

[11] OECD, Recommendation of the Council on Cross-Border Cooperation in the Enforcement of Laws against Spam [OECD/LEGAL/0344]

development of an effective international enforcement framework was regarded as a fundamental element to overcome these challenges.

Data protection is also covered by the Recommendation of the Council on High-Level Principles on Financial Consumer Protection, prepared by the Committee on Financial Markets of 2012.[12] The Recommendation explicitly mentions Responsible Business Conduct in relation to data governance. It stipulates that financial services providers and authorised agents should work in the best interest of their customers and be responsible for upholding financial consumer protection. It furthermore states that the protection of consumers' financial and personal information should be done through "appropriate control and protection mechanisms…(that) should define the purpose for which the data may be collected, processed, held, used and disclosed (especially to third parties). The mechanisms should also acknowledge the rights of consumers to be informed about data-sharing, to access data and to obtain the prompt correction and/or deletion of inaccurate, or unlawfully collected or processed data".

In 2013, the OECD revised the ***Privacy Guidelines.***[13] The revised text integrates aspects on privacy law enforcement co-operation. An important addition to the Privacy Guidelines was the introduction of the concept of a privacy management programme as a means to promote and define organisational responsibility for privacy protection ("implementing accountability"). In addition to that, the revised Privacy Guidelines integrated safeguards based on privacy risk assessment. They reflect a risk-based approach to notification in case of a security breach affecting personal data that put privacy and individual liberties at risk.

In the same period, the ***Recommendation of the Council on Health Data Governance*** [14] was adopted. This Recommendation aims to support a greater harmonisation among the health data governance frameworks of Adherents with the objective to have more countries benefit from statistical and research uses of data in which there is a public interest, and participate in multi-country statistical and research projects, while protecting privacy and data security. It refers explicitly to the MNE Guidelines.

Since 2018, the OECD is working, on the one hand towards new general principles and policy recommendations for enhanced access to public data, and on the other hand, on the implementation of the *Privacy Guidelines* in the digital environment. In this context, the OECD has concluded that the debate on data flows needs to be broadened from a focus on privacy and data protection, to an analysis that includes also data governance challenges. This requires, for example, a better understanding of the different types of data, how data are generated and collected, how different contextual factors may affect data access and sharing and data quality, data ownership, how value can be derived from data use, and how to promote mechanisms, such as data trusts, that can support the safe, fair, legal and ethical sharing (including storing) of data.

Among the OECD Recommendations applying to data governance, the Recommendation of the Council on High-Level Principles on Financial Consumer Protection and the Recommendation of the Council on Health Data Governance make explicit reference to RBC. Some aspects of data governance could need further development to which RBC standards could contribute. For example, the development of an international framework for the governance of data, might need more attention to private data (as compared to public data). Another example is the widening of the scope of data flows, for example with respect to the localisation of data, where businesses might need guidance for balancing security considerations and the need for cross border data flows.

---

[12] OECD, Recommendation of the Council on High-Level Principles on Financial Consumer Protection, [OECD/LEGAL/0394].

[13] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows and Personal Data [https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm; OECD/LEGAL/0188

[14] OECD, Recommendation of the Council on Health Data Governance [https://www.oecd.org/health/health-systems/health-data-governance.htm; OECD/LEGAL/0433].

Digital security

Another body of OECD work focuses on digital security. This work started in 1992 with the first version of the ***OECD Security Guidelines***, and has developed since then in conjunction with the *Privacy Guidelines*. Digital security is mostly covered by two OECD Recommendations: The ***Recommendation of the Council on Digital Security, Risk Management for Economic and Social Prosperity*** of 2015, and the ***Recommendation of the Council on Digital Security of Critical Activities*** of 2019.[15]

One of the recurring underlying ideas of the Recommendations is that they should contribute to continuity, resilience and safety, without inhibiting the benefits from digital transformation. Progressively, the objective of the Recommendations has shifted from raising awareness, to the protection of digital infrastructure. In addition, it takes account of the harm that digital technologies can do to other economic activities, services and functions. With that, the risk management approach to digital security has changed from a purely technical to an economic and social approach. It has resulted in the recommendation to use a "whole of government approach". Finally, cross-border digital dependencies, and the potential scope of the impact of digital failures (for example in the case of cascade failure) have gained attention and with that, the call for cross-border and multi-stakeholder co-operation has become more widely heard.

The emphasis on a multi-stakeholder approach to digital security is reflected in some explicit references made to the role of business. Although the two most recent Recommendations do not mention the MNE Guidelines, they contain a few elements that are in line with them:

- The **Recommendation of the Council on *Digital Security, Risk Management for Economic and Social Prosperity*** provides that all participants are responsible for the security of information systems and networks, hence that they should be aware of the need for security of information systems and networks and the need to enhance security, thereby respecting the legitimate interest of others who may be harmed by their action or inaction.
- The Recommendation considers the ethical conduct of business or public actors to be crucial and recommends that participants strive to develop and adopt best practices and promote conduct that recognises security needs and respects the legitimate interests of others.
- It also recommends the conduct of risk assessments at all levels of participants' activities and all aspects of their operations on a continuous basis so as to constantly deal with the evolving risks.
- The Recommendation of the Council on Digital Security of Critical Activities recognises that the consequences of digital security incidents affecting critical activities run by private operators, may extend beyond the interests of these operators, and affect a whole society and others beyond borders; and that, as a consequence, any residual risk taken by these operators may affect all those who depend on such activities as well as society as a whole.
- It furthermore recommends adhering countries to ensure that operators are responsible to manage digital security risk to critical functions with a view to protecting the continuity, resilience and safety of critical activities that they enable.

[15] OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity [OECD/LEGAL/0415], and OECD, Recommendation of the Council on Digital Security of Critical Activities[OECD/LEGAL/0456].

- Finally, it recommends adhering countries to ensure that operators effectively reduce the digital security risk to critical functions to a level acceptable for society, which should be set out in a digital security risk management policy.

Both Recommendations leave room for interpretation regarding the responsibility of, and the responsible conduct by, private operators. Where the Recommendation of 2015 does not specify the meaning of ethical conduct, the Recommendation of 2019 does not mention the concept of ethical conduct at all, and leaves its details about what is acceptable for society to national security risk management policies. This approach may result from existing differences between adhering countries in their definition of ethical conduct and/or of digital security issues and reinforces the need for international standards.

The use of digital technologies

The OECD has developed a number of Recommendations that focus on the use of digital technologies and their applications. They aim to offer guidance for policymakers in dealing with various types of challenges that these technologies and their applications may pose.

The OECD started work on AI in 2016. The resulting ***Recommendation of the Council on Artificial Intelligence***[16] adopted in 2019 represents the first international, intergovernmental standard for AI and identifies AI Principles and a set of policy recommendations for responsible stewardship of trustworthy AI. Subsequently, the G20 Leaders have welcomed G20 AI Principles, drawn from the AI Principles contained in the OECD Recommendation. The AI principles focus on responsible stewardship of trustworthy AI, and include respect for human rights, fairness, transparency and explainability,[17]robustness and safety, and accountability.

The AI Recommendation aims to complement existing OECD standards that are already relevant to AI. It refers to OECD standards in the field of privacy and data protection and digital security risk management, as well as to the MNE Guidelines and Responsible Business Conduct. There could be a role for the MNE Guidelines also with respect to the implementation of the Recommendation.

The ***Recommendation of the Council on Responsible Innovation in Neurotechnology***[18] was adopted by the OECD Council on 11 December 2019. It refers to the OECD Due Diligence Guidance for Responsible Business Conduct and the MNE Guidelines. It recommends to "promote trust and trustworthiness through norms, and practices of responsible business conduct" (art. 8e). Neurotechnology is defined as the devices and procedures used to access, monitor, investigate, assess, manipulate, and/or emulate the structure and function of the neural systems of natural persons. By converging neuroscience, engineering and AI, it is a key driver of innovation.

Apart from this positive role, neurotechnology raises ethical, legal, and societal questions such as about (brain) data privacy, the prospects of human enhancement, the regulation and marketing of direct-to-consumer devices, the vulnerability of cognitive patterns for commercial or political manipulation, and further inequalities in use and access. In order to respond to the ethical, legal and social challenges of AI, without hindering innovation, the OECD, through its Working Party on Biotechnology, Nanotechnology and Converging Technologies (BNCT), has developed a set of principles for responsible innovation in neurotechnology. It is the first international standard in this domain and aims to assist governments and innovators in addressing and anticipating the governance challenges raised by mental and neurological disorders and novel neurotechnologies.

---

[16] OECD, Recommendation of the Council on Artificial Intelligence [OECD/LEGAL/0449].

[17] i.e. by using methods and techniques whose results of the solution can be understood by humans.

[18] OECD, Recommendation of the Council on Responsible Innovation in Neurotechnology [OECD/LEGAL/0457].

Policy making in view of the digital transformation

The OECD has paid considerable attention to the development of policies that are adapted to, and help adapt to the digital transformation. A prominent one is the ***Recommendation of the Council on Principles for Internet Policy Making*** of 2011. These principles were "designed to preserve the fundamental openness of the internet, while concomitantly meeting certain public policy objectives, such as the protection of privacy, security, children online, and intellectual property, as well as the reinforcement of trust in Internet". [19] The security of the internet is presented as a condition for maintaining a level of trust and hence openness of the Internet. The principles emphasize that the policies enhancing them, should not hinder the Internet to operate.[20]

The principles make explicit reference to the Privacy Guidelines. They do not mention the MNE Guidelines. The principles for internet policy do suggest the development of codes of conduct that are supported by effective accountability mechanisms, with the aim to encourage voluntary co-operative efforts by the private sector to respect the freedoms of expression, association and assembly online, and to address illegal activity, including fraudulent, malicious, misleading and unfair practices taking place over the Internet. [21] Accountability is to be achieved through policies that make parties answerable, where appropriate, for their actions on the Internet.[22] The potential lack of attention for the negative impact in content in this Recommendation is being dealt with through the further work on Terrorist and Violent Extremist Content Online.[23]

For a long time, OECD work related to the digital transformation has focused on the development of the internet and the reduction of barriers to innovation (***Recommendation of the Council concerning Principles for Facilitating International Technology Co-operation Involving Enterprises*** of 1995, which expands on the ***Recommendation of the Council concerning a General Framework of Principles for International Co-operation in Science and Technology*** of 1988). [24] Around 2015, the OECD Recommendations in this field shifted to more attention for digital technologies, and all the actors involved in their use, ranging from government actors, non-governmental actors, businesses, citizens' associations and individuals.

In terms of policies, this meant that a whole-of-government approach became privileged. Digital technologies were increasingly considered for their positive contribution to public services and policy-making.

This was the case in the ***Recommendation of the Council on Digital Government Strategies***[25] which represented the first international legal instrument on digital government, and aimed at enhancing more strategic policy approaches for the use of technology, leading to more open, efficient, participatory and innovative governments. Relatively new was that the digital government strategies were not only considered as a contribution to economic growth as such, but were expected to create public value and mitigate risks related to the quality of public service delivery, public sector efficiency, social inclusion and participation, public trust, and multilevel and multi-actor governance. This shift in focus brought about more attention for ethical considerations related to the use of digital technologies.

---

[19] OECD, Recommendation of the Council on Principles for Internet Policy Making [OECD/LEGAL/0387], p.7.

[20] Idem, p.26

[21] Idem, p.23

[22] Idem, p.24

[23] See also the most recent OECD digital economy paper no. 296: "Current approaches to terrorist and violent extremist content among the global top 50 online content-sharing services" (August, 2020).

[24] OECD, Recommendation of the Council concerning Principles for Facilitating International Technology Co-operation Involving Enterprises [OECD/LEGAL/0282]; OECD, Recommendation of the Council concerning a General Framework of Principles for International Co-operation in Science and Technology [OECD/LEGAL/0237].

[25] OECD, Recommendation of the Council on Digital Government Strategies [OECD/LEGAL/0406].

In the ***Daejeon Declaration on Science, Technology and Innovation Policies for the Global and Digital Age*** adopted in 2015,[26] science technology and innovation were said to foster sustainable economic growth, job creation and enhanced well-being. It aimed to promote the formulation of new, and the adaptation of the existing, science, technology and innovation (STI) policies, in order to harness the benefits and to address the policy challenges brought about by the digitalisation of STI. The Declaration underlined the importance of rule setting and governance mechanisms to better exploit open science, invest in global research infrastructures, and accelerate collective responses to crises, also in relation to emerging and less developed countries. It furthermore mentioned the positive contribution STI could have, not only for sustainable economic growth, but also for a cleaner environment and a more inclusive society.

In June 2016, a similar message was issued by the ***Declaration on the Digital Economy: Innovation, Growth and Social Prosperity*** *(Cancún Declaration).*[27] It furthermore promoted digital security risk management and the protection of privacy, accountability and transparency. It declared to support the development of international arrangements that promote effective privacy and data protection across jurisdictions, including through interoperability among frameworks. There is no reference to the MNE Guidelines in the Declaration.

Consumer protection in E-commerce

The digital transformation has had an important impact on individuals as consumers of internet content of the Internet of Things, as providers of data, as actors in e-commerce transactions etc. This has increased the need for clear rules in order to protect them. In 2016, the ***Recommendation of the Council on Consumer Protection in E-commerce***[28] (i.e. business-to-consumers and consumers-to-consumers transactions that are facilitated by internet) was adopted on the proposal of the Committee on Consumer Policy (CCP). It replaced the 1999 OECD Recommendation on Consumer Protection in E-commerce. The Recommendation of 2016 sets out the core characteristics of consumer protection in e-commerce that should be in place in countries and addresses some of the key developments in e-commerce since 1999, including emerging challenges associated with consumer ratings and reviews, the use of consumer data, and product safety. It recommends that adhering countries work with businesses, consumer representatives and other civil society organisations in a transparent and inclusive manner to implement a set of principles and their policy frameworks for the protection of consumers in e-commerce. These principles tackle issues such as fair business, advertising and marketing practices, online disclosures and dispute resolution.

In addition to the principles, the Recommendation deals with their implementation and mechanisms to enhance trust in e-commerce, including through the promotion of effective dispute resolution.[29] It emphasises the importance to co-operate and work toward developing agreements or other arrangements for the mutual recognition and enforcement of judgments resulting from disputes between consumers and businesses, and judgments resulting from law enforcement actions taken to combat fraudulent, misleading or unfair commercial conduct. The Recommendation also calls for the development and enforcement of joint initiatives at the international level among governments and stakeholders. Although the Recommendation does not refer to the MNE Guidelines, the promotion of effective dispute resolution is highly relevant from an RBC perspective and NCPs may refer to the Recommendation when applying Chapter VIII (Consumer Interests) of the MNE Guidelines.

[26] OECD, Daejeon Declaration on Science, Technology and Innovation Policies for the Global and Digital Age [OECD/LEGAL/0416].
[27] OECD, Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration) [OECD/LEGAL/0426].
[28] OECD, Recommendation of the Council on Consumer Protection in E-commerce [OECD/LEGAL/0422].
[29] This topic is also under debate in the WTO, in the Work Programme on Electronic Commerce, see section 3.

Digital technologies and the environment

In 2010, the Council adopted the ***Recommendation of the Council on Information and Communication Technologies and the Environment***[30] on the proposal of the Committee on Digital Economy Policy. The Recommendation aims to support national efforts to establish, improve and review policies on information and communication technologies (ICTs) and the environment. It stipulates to reduce the direct effects of ICTs themselves on the environment, to enable the effects of ICT applications in other sectors, and the systemic effects to change social and cultural behaviour through the use of ICTs. Many of the principles underlying the considerations for the adhering countries in the Recommendation correspond to similar recommendations for enterprises, (albeit not specifically focused on digitalisation) in Chapter VI of the MNE Guidelines (Environment). Examples are the recommendation to develop resource-efficient ICTs, the promotion of widespread development and adoption of clear standards or eco-labels, and awareness raising among the users/consumers about the environmental implications of the use of ICT/products and services.

The Recommendation furthermore instructs adhering countries to enhance the positive effects of information and communication technologies on the environment. For example, governments should help create an environment that helps businesses in seizing the opportunities of digital technologies to address the SDGs, and to green the economy. It underscores the importance of monitoring compliance with the policies and setting clear responsibilities. In the Recommendation, the potential negative impacts that digital technologies may have on the environment, for example through energy intensive practices like cloud computing, receive less attention. In addition, the Recommendation looks at ICT and not on other aspects of digitalisation. There seems thus to be some margin for further development of principles for the greening of digital consumption (either by consumers or through business accountability).

Taxation and digitalisation

Since 2015, the OECD has been working on ways to tackle some challenges for tax rules related to the digitalisation of the economy, as one of the main areas of focus of the Base Erosion and Profit Shifting (BEPS) Action Plan. Digitalisation fundamentally challenges the rule based international tax system based on jurisdiction for non-resident companies, as companies increasingly do business with customers in jurisdictions without having a physical presence there (for example, in the case of e-commerce).

In May 2019, the 130 members of the OECD/G20 Inclusive Framework on BEPS approved the *Programme of Work to Develop a Consensus Solution to the Tax Challenges Arising from the Digitalisation of the Economy*, laying out a process for reaching a new global agreement for taxing multinational enterprises.

This programme looks into the allocation of taxing rights while taking into account the profit allocation and nexus rules, on the one hand. On the other hand, it seeks to develop rules that are designed to ensure that a multinational enterprise is subject to a minimum level of tax on its profits.[31]

[30] OECD, Recommendation of the Council on Information and Communication Technologies and the Environment [OECD/LEGAL/0380].

[31] Programme of Work to Develop a Consensus Solution to the Tax Challenges Arising from the Digitalisation of the Economy, OECD/G20 Inclusive Framework on BEPS, OECD, Paris, https://search.oecd.org/tax/programme-of-work-to-develop-a-consensus-solution-to-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.htm

The MNE Guidelines encourage companies to design their tax oversight and tax compliance in a responsible manner, and to comply with both the letter and spirit of the tax laws and regulations of the countries in which they operate. So far, few specific instances related to tax evasion or tax avoidance have been filed with the NCPs (a submission against Glencore International AG and First Quantum Mining Ltd. filed with, and concluded by, the Swiss and Canadian NCPs in 2012; a submission by FNV against Chevron that was filed with the Dutch NCP in 2018; and a specific instance by A*h*Top against AirBnB, filed with the French NCP in 2020).

From this overview of OECD standards related to digitalisation, the following trends emerge: There has been a shift from a focus on policies dealing with one aspect of digitalisation, such as internet policies or cybersecurity, to more attention for a whole-of-government approach, a multi-stakeholder approach, and the need for cross-border co-operation. With this development, the role of business and its responsibilities, have received more attention. A broadly accepted way of dealing with the responsibilities of these stakeholders has become risk management. Digital risks have come to be considered an integral part of an organisation's overall risk management and decision-making process. Parallel to that, the impact of digitalisation on the well-being of individuals and on society as a whole has gradually come to the forefront. This has led to more attention for human rights in digitalisation, for example in the case of digital security. Disclosure has also become a recurrent topic, for example in the case of data governance or AI. Questions about the extent to which digitalisation is fair, inclusive or ethical have become more prominent as was observed in relation to online content and its users and consumers, or the business models that develop thanks to digitalisation.

These trends are reflected, on the one hand, in some Recommendations on digitalisation which explicitly refer to the MNE Guidelines and have integrated aspects of Responsible Business Conduct. This is the case for *the Recommendation on High-Level Principles on Financial Consumer Protection (2012); the Recommendation on Health Data Governance* (2016); *the Principles for Trustworthy AI (2019)*; and the *Recommendation on Responsible Innovation in Neurotechnology (2019).* There are also Recommendations that do not explicitly refer to the MNE Guidelines but use wording linked to responsible business conduct, such as *accountability*, *fair business* (*Recommendation on Consumer Protection in E-commerce*), and *ethical conduct (Recommendation on Digital Security Risk Management for Economic and Social Prosperity*).

Looking ahead, the MNE Guidelines have an important role to play with regard to digitalisation. Options for future developments vary from including references to the MNE Guidelines in new legal instruments and policy initiatives; including specific language on digitalisation in a future review of the MNE Guidelines; and developing additional guidance and tools for governments and business.

International and regional initiatives regarding digitalisation

This subsection provides an overview of other initiatives at international and regional levels. The overview is based on desk research and is not intended to be exhaustive.

European Union

In May 2018, the European *General Data Protection Regulation (GDPR)*[32] has come into force. The regulation contains provisions and requirements related to the processing of personal data of individuals and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects inside the European Economic Area. This regulation has unified regulation within the EU, which has made it easier for companies to comply with it within the EU. In addition to this, the ECJ rulings about GDPR issues give guidance to business, for example in response to two cases dealing with the "right to be forgotten".[33] The GDPR also applies to the transfer of personal data outside the EU.

Over the last 6 years, and in addition to the GDPR, the European Union has taken various steps towards the regulation of the digital economy. Examples are the Regulation on the free flow of non-personal data, the Cybersecurity Act, and the Open Data Directive.

In 2018, the EU presented a Strategy for AI. It includes the elaboration of recommendations on future-related policy development and on ethical, legal and societal issues related to AI, including socio-economic challenges. The Strategy has resulted, among other things, in the Policy and Investment Recommendations, which require accountability complements and the reporting about negative impacts; and the Ethics Guidelines for Trustworthy Artificial Intelligence (AI) (revised document of April 2019). These non-binding guidelines address, among other things, accountability and risk assessment, privacy, transparency, societal and environmental well-being. In February 2020, the European Commission issued a White Paper[34] and an accompanying Report on the safety and liability framework, which set out policy objectives on how to achieve a regulatory and investment oriented approach that both promotes the uptake of AI and addresses the risks associated with certain uses of AI at the same time.

In 2020, the European Commission presented an overall strategy for data and artificial intelligence (conclusions adopted by the Council in June 2020). Besides the aforementioned work on AI, the *EU Digital Strategy* covers many issues, ranging from connectivity, digital value chains, and eHealth, to the data economy, and digital platforms. It focuses on building a value-based and inclusive digital economy and society, and an open but rules-based market, and aims to contribute to an open, democratic and sustainable society.[35]

---

[32] EU Regulation 2016/679 (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), https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04.

[33] European Union Court of Justice Ruling (2019) C-136/17, http://curia.europa.eu/juris/document/document.jsf?docid=218106&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=969167 and European Union Court of Justice Ruling (2019) C-507/17 http://curia.europa.eu/juris/document/document.jsf?docid=218105&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=969325

[34] European Commission (2020), "White Paper On Artificial Intelligence - A European approach to excellence and trust", Brussels, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[35] European Commission (2020), "Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence", Brussels, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273.

The EU furthermore envisages to set up a European data space, for which it prepares a regulatory framework regarding data governance, access to, and the (re)use of data between businesses, between business and government, and within administrations.

Also as part of the EU Digital Strategy, the European Commission is preparing the *Digital Service Act package*. It aims to update the *E-Commerce Directive* (in place since 2000), by addressing the safety of users online, and the development of new digitally-based business models. This work is supported by the *Platform to Business Regulation*, which entered into force in July 2020. It aims to protect (smaller) businesses and traders relying on search engines and online platforms, by focusing on fairness, transparency, and predictability.[36] In addition, the European Commission is expected to further develop the existing general guidelines (a Communication in 2017 and a Recommendation in 2018) to online platforms and Member States for tackling illegal content online.[37]

Council of Europe

In 1981, the Council of Europe adopted *Convention 108 for the Protection of Individuals with regard* to Automatic Processing of Personal Data. This Convention went into force five years after the OECD Privacy Guidelines, and constitutes the first binding international instrument for the protection of individuals against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the cross border flow of personal data. Parallel to the OECD revision of the Privacy Guidelines, the Council of Europe modernised Convention 108 in order to enhance its implementation and to adapt it to new technological developments. During this process and until its completion in 2018, the OECD was strongly involved. The modernisation also took account of the EU data protection rules that later culminated in the adoption of GDPR legislation, and consulted with some non-Member States. Convention 108+, the updated version, contains some changes in the terminology and scope (for example, with regard to the processing of data) and new insights. Examples are the attention for the positive effect of processing of personal data on other fundamental rights of individuals. An important new aspect of the modernised Convention is that it gives states that do not fall under the Council of Europe, and other International Organisations (and the EU), the possibility to accede to the Convention.

In addition to Convention 108, in September 2019 the Ministers of the Council of Europe have set up an intergovernmental *Ad hoc Committee on Artificial Intelligence* (CAHAI), to examine the feasibility of a legal framework for the development, design and application of artificial intelligence. Important issues to be addressed include the need for a common definition of AI, the mapping of the risks and opportunities arising from AI, notably its impact on human rights, rule of law and democracy, as well as the opportunity to move towards a binding legal framework. It takes due account of a gender perspective, building cohesive societies and promoting and protecting rights of persons with disabilities in the performance of its tasks.

Furthermore, the Council of Europe has, in the past years, developed a number of non-binding standard setting instruments on the roles and responsibilities of private actors with regard to the respect of human rights online, such as the Recommendation CM / Rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.[38]

[36] European Commission (n.d.), "Platform-to-business trading practices", Brussels, https://ec.europa.eu/digital-single-market/en/business-business-trading-practices.

[37] European Commission (2018), European Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online, https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

[38] See list of adopted Committee of Ministers texts on media and information society, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts.

Most recently, in April 2020, the Council of Europe´s Committee of Ministers issued a set of guidelines calling on governments to ensure that they do not breach human rights through their own use, development or procurement of algorithmic systems.[39] The recommendation calls on governments to establish effective and predictable regulatory frameworks that prevent, detect, prohibit and remedy human rights violations, whether stemming from public or private actors.

United Nations

The ***UN Human Rights Business and Human Rights in Technology (B-Tech) Project*** seeks to provide authoritative guidance and resources to enhance the quality of implementation of the United Nations' Guiding Principles on Business and Human rights with respect to a selected number of strategic focus areas in the technology space.[40] It aims to offer practical guidance and public policy recommendations to realise a rights-based approach to the development, application and governance of digital technologies. It uses an approach that includes attention for human rights risks, corporate responsibility and accountability by using the three pillars of the UNGPs: Protect, Respect, and Remedy. For example, it looks at the role of states and private actors in enhancing human rights in business models, human rights due diligence, and accountability and remedy. The project offers a framework for what responsible business conduct looks like in practice, regarding the development, application, sale and use of digital technologies and suggests a smart mix of regulation, incentives and public policy tools for policy makers that provide human rights safeguards and accountability, without hampering the potential of digital technologies to address social, ecological and other challenges.

Other UN-related work with a focus on the internet is done in the framework of the ***Internet Governance Forum***,[41] a UN-mandated forum for multi-stakeholder policy dialogue that seeks to enhance a dialogue between policy makers and the internet community. It started in 2005 (with a mandate now extended to 2025), with a request by the *World Summit on the Information Society* (WSIS) for a broad based discussion of public policy issues in relation to the internet. The Forum aims to facilitate a common understanding of how to maximize internet opportunities, to address risks and challenges that arise from the internet, and to build capacity in developing countries. In 2019, one of the themes discussed was data governance and approaches to ensure the development of human-centric data governance frameworks. Another track focused on digital inclusion and the improvement of access to equitable opportunities in the digital age. A third theme dealt with security, safety, stability and resilience.[42] Within the overarching theme of "Internet for human resilience and solidarity", the current themes for 2020 are data, environment, inclusion and trust, based on the outcome of 2019 and a comprehensive stakeholder consultation.[43]

---

[39] 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, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

[40] See OHCHR webpage on the B-Tech Project for full list of materials, https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.

[41] United Nations Internet Governance Forum (2014),"The Global Multistakeholder Forum for Dialogue on Internet Governance Issues", *United Nations*, http://intgovforum.org/cms/2014/IGFBrochure.pdf.

[42] United Nations Internet Governance Forum (2019), "IGF 2019 Themes", *United Nations*, https://www.intgovforum.org/multilingual/content/igf-2019-themes.

[43] United Nations Internet Governance Forum (2020), "IGF 2020 Themes", *United Nations*, https://www.intgovforum.org/multilingual/content/igf-2020-thematic-tracks.

In 2015, UNESCO adopted the ***ROAM principles*** (Rights, Openness, Access and Multi-stakeholder governance) which are part of the concept of ***Internet Universality Indicators***. This is a research tool to holistically assess the state of internet development nationally through a set of 303 indicators covering six categories. In relation with internet issues, UNESCO is also working on Artificial Intelligence on the basis of the same ROAM principles, as well as on broadband and the ethical aspects of digitalisation. The ***World Commission on the Ethics of Scientific Knowledge and Technology*** **(COMEST)** has carried out work on ethical issues relating to the technologies of the information society. In 2017, it has issued a publication on Robotics Ethics about the accountability of actions of cognitive machines and their impact on human behaviours, inducing social and cultural changes, and on issues related to safety, privacy and human dignity. Under UNESCO's intergovernmental *Information for All Programme* (IFAP), a ***Code of Ethics for the Information Society*** has been developed.

Although not specifically focused on RBC, it is worth mentioning the UN General Assembly Resolution on Information and Communications Technologies for Sustainable Development[44] acknowledging the role this technology has in achieving Sustainable Development Goals. The UN Secretary-General's High-level Panel on Digital Cooperation also issued a recent report on how digital cooperation can contribute to the achievement of the Sustainable Development Goals.[45]

World Trade Organisation (WTO)

In 1998, WTO ministers adopted the ***Declaration on Global Electronic Commerce*** and subsequently established a ***Work Programme on e-commerce***. It aimed to examine all trade-related issues relating to global electronic commerce resulting in a WTO agreement on e-commerce. Discussions have continued and focus mostly on how to remove further barriers to e-commerce, without increasing the divide between leaders and laggards. During the World Economic Forum in Davos in January 2019, the negotiations received a new impetus with the decision by the EU and 48 members of the WTO to start negotiations about global rules on electronic commerce. The G20 (Osaka Meeting in 2019) gave this a boost, followed by an agreement in Davos (January 2020) between 83 trade ministers to present a consolidated negotiating text at the 12th Ministerial Conference of the WTO, to be held in Kazakhstan in June 2021.

International Labour Organization (ILO)

The discussions on digitalisation at the ILO centre around enhancing decent work. In 2019, the ILO presented the ***Agenda for the Future of Work.***[46] The ILO Centenary Declaration for the Future of Work, adopted at the International Labour Conference in 2019, addressed some key challenges in relation to the use of (digital) technology in support of decent work and declared that efforts were to be directed to harnessing the fullest potential of technological progress and productivity growth to achieve decent work and sustainable development.

[44] United Nations General Assembly Resolution A/RES/74/197 (2019) on Information and communications technologies for sustainable development, https://undocs.org/en/A/RES/74/197.

[45] UN Secretary-General's High-level Panel on Digital Cooperation (2019), "The Age of Digital Interdependence", *United Nations*, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

[46] ILO (2019) "Work for a brighter future – Global Commission on the Future of Work", *ILO*, https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_662410.pdf.

The Agenda for the Future of Work is based on three pillars: Firstly, it calls for the adoption of a "human-in-command" approach to artificial intelligence that ensures that the final decisions affecting work are taken by human beings. Secondly, it aims at the development of an international governance system for digital labour platforms that requires platforms (and their clients) to respect certain minimum rights and protections. Thirdly, it raises the importance of developing more regulation of data use and algorithmic accountability in the world of work.

In 2018, the ILO published a report on working conditions at five of the major, global, online micro-task platforms.[47] It is based on an ILO survey covering 3,500 workers in 75 countries around the world and other qualitative surveys. The report analyses the working conditions on these micro-task platforms, including pay rates, work availability and intensity, social protection coverage and work–life balance. The report recommends 18 principles for ensuring decent work on digital labour platforms.

Asia-Pacific Economic Cooperation (APEC)

An example of an interregional initiative dealing with digitalisation is the **APEC Roadmap on Internet and Digital Economy** of 2017. It provides guidance on key areas and actions to facilitate technological and policy exchanges among member economies, and to promote innovative, inclusive and sustainable growth, as well as to bridge the digital divide in the APEC region. The roadmap underlines the importance of a holistic approach to the development of government policy frameworks for the Internet and Digital Economy.

[47] Berg, J. et al, (2018), "Digital labour platforms and the future of work", *ILO*, https://www.ilo.org/global/publications/books/WCMS_645337/lang--en/index.htm.

3. National, industry and stakeholder standards and initiatives

This section seeks to provide a high-level mapping and snapshot of national and industry standards and initiatives concerned with RBC governance issues in the digital transformation. Specifically, the mapping assesses the efforts by states, civil society, multi-stakeholder initiatives, and companies to deal with the RBC aspects of digitalisation, in particular with respect to AI and online platforms".[48] Furthermore, it identifies key trends across a range of actors, and presents certain gaps in governance and best practice guidance for what concerns the RBC aspects of digitalisation and digital transformation.

Due to resource and time limitations, the list of efforts is non-exhaustive and relies mostly on secondary sources. Only documents with accessible English translations were assessed. Furthermore, while global in scope, it primarily features initiatives from developed countries or companies headquartered in developed countries. Stakeholder initiatives in this space are rapidly evolving and may not fully and neatly fit into specific categories. More in-depth research may be required for a comprehensive stocktaking that would also present a comprehensive qualitative assessment, fully identify gaps, and present recommendations.

Methodology and Scope

The mapping examines four groups of stakeholder initiatives (state, civil society, multi-stakeholder, and company) in relation to the nine chapters of the MNE Guidelines[49] to identify if the issues contained in the chapters were mentioned and addressed by the initiatives. It also maps the extent to which initiatives are concerned with AI or social media platform issues, international instruments were referenced, and the extent to which oversight mechanisms are in place. Finally, the mapping examines company AI principles and ethics efforts to see whether they address the six steps of the due diligence process.[50]

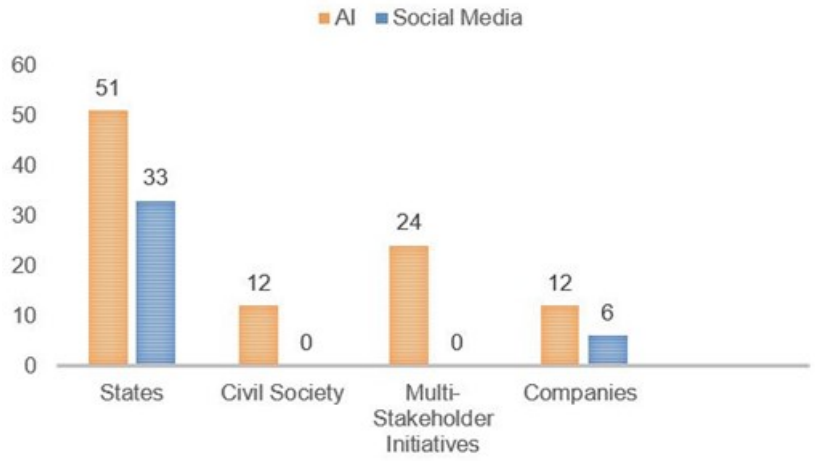
All initiatives discussed below are listed in more detail in the Annex:

[48] This mapping was supported by *Article One*. *Article One* is a consultancy that works with companies, multilateral institutions, and state agencies, to help its clients develop and implement strategies to promote respect for human rights and advance sustainability. https://www.articleoneadvisors.com/

[49] The nine substantive chapters of the MNE Guidelines are: Disclosure, Human Rights, Labour Rights, Environment, Bribery, Consumer Interests, Science & Technology, Competition, and Taxation.

[50] The six steps of OECD due diligence process are: 1. Embed RBC into Policies & Management, 2. Identify & Assess Adverse Impacts in Operations, Supply Chains & Business Relationships, 3. Cease, Prevent or Mitigate Adverse Impacts, 4. Track Implementation & Results, 5. Communicate How Impacts are Addressed, and 6. Provide for or Cooperate in Remediation.

Figure 3.1. Total number of initiatives reviewed for this study



Note: The table represents the total number of initiatives reviewed for this study, broken down by stakeholder group.

State driven initiatives:

- Legislation that is currently enacted or going through legislative processes to provide a global overview of how states are protecting or impacting digital rights;
- National strategies focused on AI readiness and/or Social Media regulations;
- Research and nationally sponsored recommendations that showcase the states' cross-sector collaboration with industry and civil society, and long-term investment in the digital economy.

Multi-stakeholder initiatives:

- Company and civil society partnerships that highlight corporate alignment with rights respecting RBC principles outside of government regulation, working directly with civil society;
- Whitepapers and recommendations by the OECD and the UN that contribute to corporate and state best practices.

Civil society initiatives:

- Voluntary initiatives focused largely on cross-sector collaboration;
- Whitepapers and recommendations by NGOs and academic institutions that demonstrate how civil society is shaping national approaches to the digital economy, and helping to establish global norms;
- Ratings and rankings showing increased attention of operationalization of principles.

Company initiatives:

- Company AI Ethics and Guiding Principles outlining commitments to rights holders across many applications of AI;
- Social Media community guidelines and standards outlining content moderation efforts by companies.

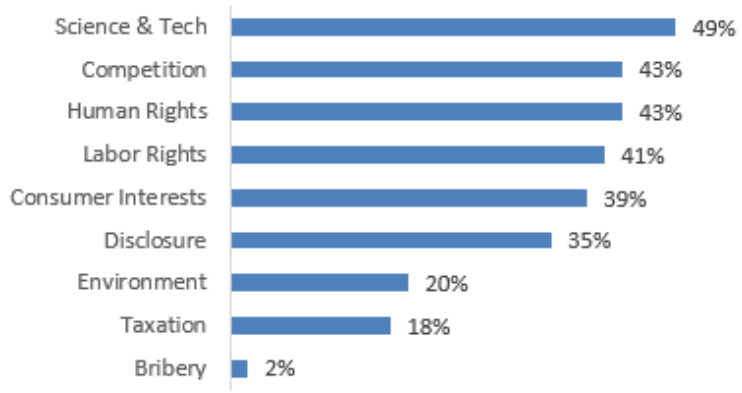
Research Findings

This section summarises the research findings across initiatives of the four stakeholder groups. They showcase the types of efforts undertaken by each stakeholder group and, where relevant, the links to the chapters of the MNE Guidelines.

State initiatives

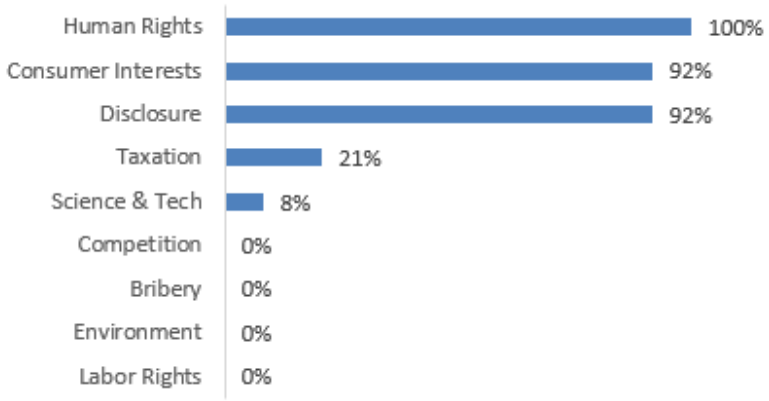
Figures 3.1 and 3.2 show the percentage of AI initiatives related to RBC issues[51] and social media legislation related to RBC issues respectively, that include content related to the MNE Guidelines' chapters.

Figure 3.2. Overview of government AI initiatives related to RBC issues by theme



Note. Based on an assessment of strategies in 51 jurisdictions.

Figure 3.3. Assessment of government social media legislation related to RBC issues by theme

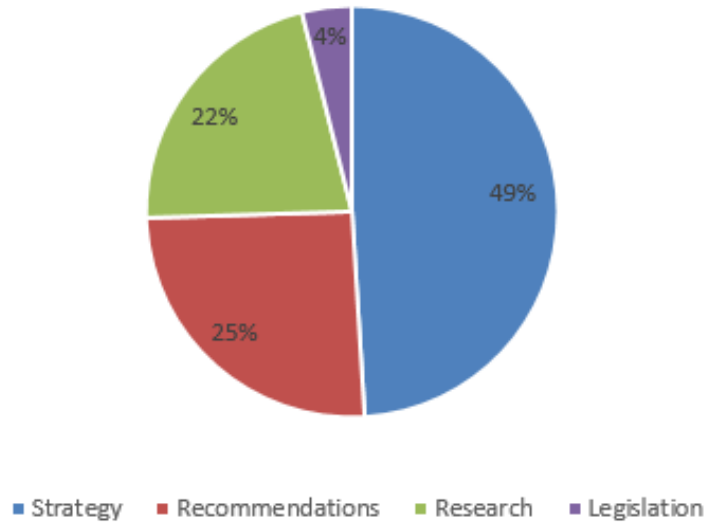


Note. Based on an overview of social media legislation efforts in 25 jurisdictions.

[51] These figures were developed for the draft of the document presented to the Working Party on Responsible Business Conduct in March 2020. Subsequently, two additional state efforts were identified, as were three additional multi-stakeholder initiatives. Nonetheless, the percentages presented in the figures remain roughly the same.

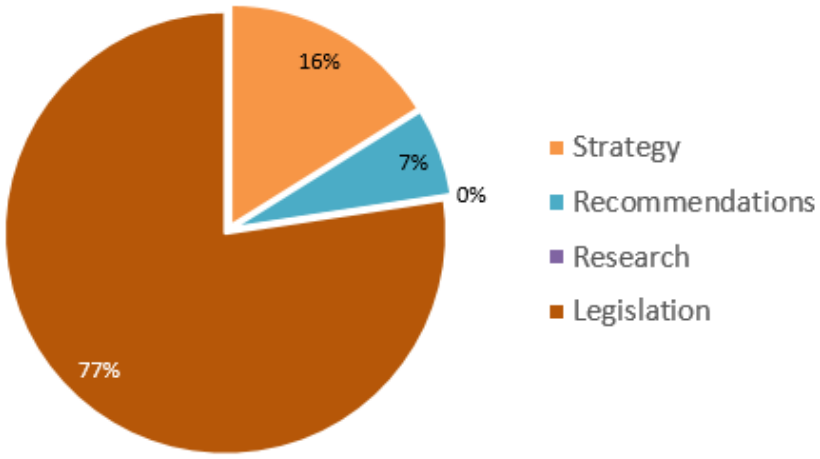
Subsequently, the types of initiatives undertaken by States on the governance of AI (Figure 3.4) and Social Media (Figure 3.5) were examined. These were grouped into four categories and involve legislation, recommendations, research, and strategy:

Figure 3.4 Assessment of government AI initiatives by type



Note. Based on an assessment of AI initiatives in 51 jurisdictions.

Figure 3.5 Overview of government social media initiatives by type

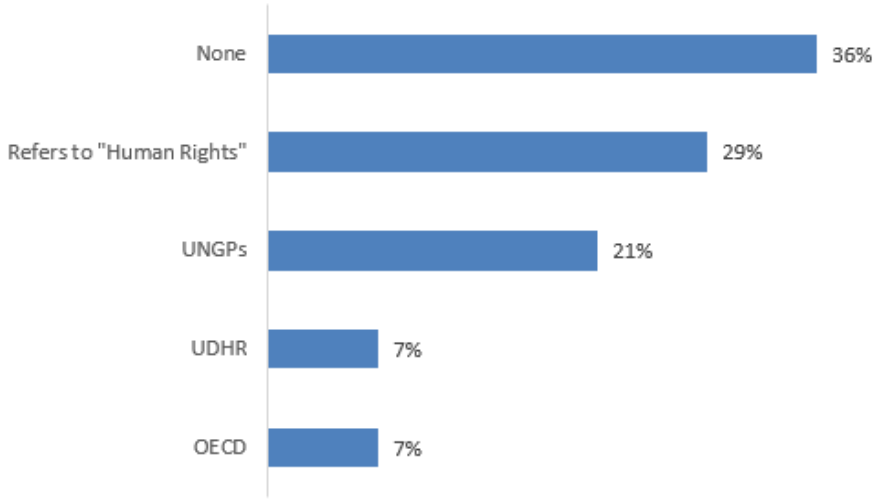


Note. Based on an overview of social media initiatives in 31 jurisdictions.

Civil Society Initiatives

Civil society organisation (CSO) publications were reviewed to identify what international standards they may reference.[52] (Figure 3.6):

Figure 3.6 References to international standards in CSO publications



Note. Based on an overview of 12 CSO publications.

Multi-Stakeholder Initiatives

The assessment of multi-stakeholder initiatives, consisted of 16 company and civil society partnerships, and publications by the OECD and the UN. The assessment concluded that multi-stakeholder initiatives have driven voluntary approaches to corporate governance. Key initiatives include:

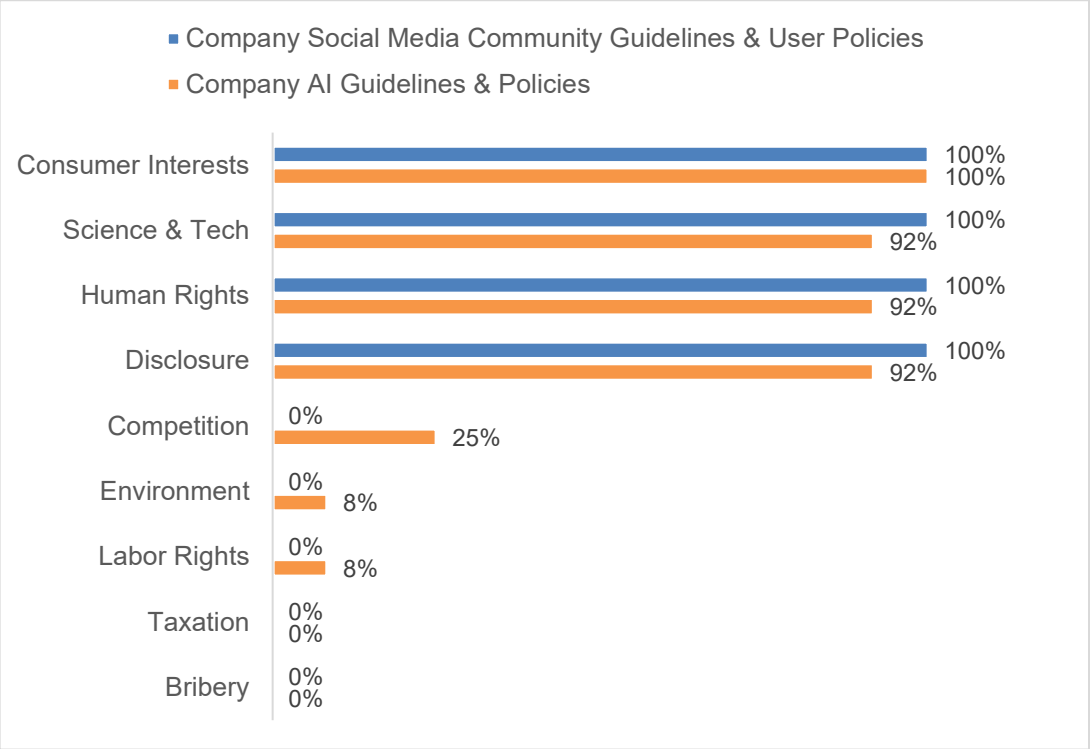
- The *Global Network Initiative* principles which provides high-level guidance to the ICT industry on how to respect, protect, and advance user rights to freedom of expression and privacy;
- The *Christchurch Call* which outlines commitments from Governments and online service providers, intended to address terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in, and after the Christchurch attacks;
- The *Partnership on AI* which primarily focuses on stakeholder engagement and dialogue, seeking to maximise the potential benefits of AI for as many people as possible.

[52] Leading CSO efforts include: the *Santa Clara Principles* which call for transparency from Social Media companies by publishing the numbers of removed posts, notifying users of content removal, and providing opportunities for meaningful and timely appeals; the *Toronto Declaration* which is a human rights-based framework that delineates the responsibilities of States and private actors to prevent discrimination with AI/ML advancements; and *Ranking Digital Rights* which is the first public tool to assess company performance on digital rights – working to trigger a 'race to the top.'

Company initiatives

Figure 2.6 shows a mapping of company initiatives concerning social media community guidelines and user Policies, and AI guidelines and policies in relation to the MNE Guidelines chapters.

Figure 3.7 Overview of company initiatives governing social media and AI



Note. This overview covers the initiatives of selected companies in relation to OECD Guidelines chapters.

ANNEX: Mapping of standards and initiatives

This Annex organises and maps out all the standards and initiatives discussed and counted in the sections of the paper above. The table is organised by firstly, listing government efforts on AI and Online Platforms, and secondly by breaking them down into legislation, recommendations, research, and strategy. This is followed by additional tables on civil society and multi-stakeholder initiatives, then industry-led initiatives, organised as best practice guidance, ratings and rankings, and voluntary initiatives.

Artificial intelligence initiatives by country/territory/organisation/region

	Overview	RBC Issues Covered	Reference to International Instruments
LEGISLATION			
Chile	Chile is developing a *National AI Policy* to be released in 2020. The Ministry of Science, Technology, Knowledge, and Innovation created a committee of ten experts to lead the effort. Information provided by: https://oecd.ai/dashboards/countries/Chile	*Human Rights, Labour Rights, Consumer Interests, Science and Technology Competition*	*No*
European Union	The EU's General Data Protection Regulation (GDPR) establishes new protections for European citizens' rights around data protection and privacy, which impacts any organization collecting European residents' data. Information provided by: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en	*Privacy, Transparency, Informed Consent, Safety, Security*	*No*
RECOMMENDATIONS			
People's Republic of China (China)	In June 2019, the New Generation AI Governance Expert Committee (established by MOST) released principles of next-generation AI governance. Information provided by: https://oecd.ai/dashboards/countries/China	*Disclosure, Human Rights, Consumer Interests, Science and Technology, Competition*	*No*
Council of Europe	Council of Europe's *Artificial Intelligence and Data Protection* establishes that AI development relying on the processing of personal data should be based on the principles of Convention 108+. Information provided by: https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection	*Disclosure Human Rights, Consumer Interests, Science and Technology*	*No*
	In 2019, the Council of Europe issued a recommendation on AI and human rights, titled *Unboxing Artificial Intelligence: 10 steps to protect Human Rights*. Information provided by:	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology*	*No*

	Overview	RBC Issues Covered	Reference to International Instruments
	https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights		
	The Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes is a commitment by Member States to uphold the rights and freedoms enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms offline and online. The declaration addresses "contemporary machine learning tools have the growing capacity not only to predict choices but also to influence emotions and thoughts and alter an anticipated course of action, sometimes subliminally." Information provided by: https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b	*Human Rights Consumer Interests Science and Technology*	*No*
European Commission	European Commission welcomed the final Ethics Guidelines for Trustworthy Artificial Intelligence prepared by the High-Level Group on Artificial Intelligence published on 8 April 2019. The European Commission also welcomed the Report on liability for Artificial Intelligence and other emerging technologies prepared by the Expert Group on Liability and New Technologies published on 21 November 2019. Information provided by: https://oecd.ai/dashboards/countries/EuropeanUnion	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
Estonia	In 2019, Estonia AI experts put together a report outlining valuable advice and activities on how to accelerate applying AI in private and public sectors. The report concluded that there was no need for changes in the foundation of the Estonian legal system, nor for a unified AI law. The report recommended some laws be modernised to apply to AI in business, to create more general awareness, research, development and innovation rather than sector specific prioritization. In May 2019, the Estonian government has launched a national AI strategy. Information provided by: https://oecd.ai/dashboards/countries/Estonia and https://e-estonia.com/estonia-accelerates-artificial-intelligence/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology*	*No*
France	In 2017, France's "AI for Humanity" national strategy launched a mission delegated to Mathematician Cédric Villani by the French prime Minister to assess the French AI Strategy. Villani's report, "For a Meaningful Artificial Intelligence," was published in 2018. Information provided by: https://oecd.ai/dashboards/countries/France	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology*	*No*
Germany	The government established a new Data Ethics Commission which released recommendations for the government and other institutions for ethical AI in October 2019. The independent Commission called for AI to be designed safely and securely, to respect people's rights and freedoms, protect democracy, and avoid bias and discrimination. It also argued that lethal autonomous weapons should be banned outright. Information provided by: https://oecd.ai/dashboards/countries/Germany	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology*	*No*
Italy	In 2017 the Agency for Digital Italy launched an AI task force (AGID) of 30 direct members and around 450 community members from many sectors. In 2018, AGID released a White Paper called "AI at the service of citizens," that recommended how to develop better public services with the use of AI that could help eliminate inequalities and measure impact. Italy is also coordinating the Thematic Group on Emerging Technologies (AI and Blockchain) of the OECD Working Party of Senior Digital Government Officials. Information provided by: https://oecd.ai/dashboards/countries/Italy	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*
Japan	In 2017 Japan published Draft AI Research and Development Guidelines for International Discussions in preparation for the Conference toward AI Network Society. The draft document is a set of non-binding AI RandD principles and	*Disclosure, Human Rights, Consumer Interests*	*No*

	Overview	RBC Issues Covered	Reference to International Instruments
	guidelines regarding the promotion of the benefits and the reduction of the risks of AI. Information provided by: https://oecd.ai/dashboards/countries/Japanhttps://futureoflife.org/ai-policy-japan/		
Kenya	The Kenyan government created a Blockchain and Artificial Intelligence task force in February 2018 consisting of 11 members from academia and industry. The first goal of the group is to provide the government with recommendations about how to harness these emerging technologies over the next five years. Information provided by: https://futureoflife.org/ai-policy-Kenya/	*Disclosure, Human Rights, Labour Rights, Consumer, Interests, Science and Technology, Competition*	*No*
Norway	In 2018, the Norwegian Data Protection Authority published a report elaborating on its legal opinions and the technologies described in the 2014 report "Big Data – data protection principles under pressure," providing greater technical detail in describing AI, while also taking a closer look at four relevant AI challenges associated with the data protection principles embodied in the GDPR. Information provided by: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf	*Disclosure, Consumer Interests, Science and Technology*	*No*
United Kingdom	In 2018, the Select Committee on AI published a 183-page report, "AI in the UK: ready, willing and able?" which considers AI development and governance. It acknowledges that the UK cannot compete with the US or China in terms of funding or people, but suggests the UK may have a competitive advantage in considering the ethics of AI. The government responded to the report's recommendations in a 41-page document highlighting many of the UK's intentions moving forward. Information provided by: https://www.gov.uk/government/publications/ai-in-the-uk-ready-willing-and-able-government-response-to-the-select-committee-report	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*
	In 2017, an All-Party Parliamentary Group on Artificial Intelligence (APPG AI) was established to address ethical issues, social impact, industry norms, and regulatory options for AI in Parliament. The group's first findings are described in: "1 Key Recommendation, 6 Policy Focus Areas." The key recommendation is to appoint a Minister for AI in the Cabinet Office. Information provided by: https://www.appg-ai.org	*Human Rights, Labour Rights, Science and Technology, Competition*	*No*
RESEARCH			
Austria	Austria has the Austrian Society for Measurement, Automation, and Robotics Technology, which established the National Robotics-Technology Platform (GMAR) in 2015, supported by the Austrian Ministry of Transport, Innovation and Technology. Information provided by: https://produktionderzukunft.at/en/platforms/gmar.php	*Labour Rights, Science and Technology, Competition*	No
	Austria established a Robot Council in 2017, an advisory body for current and future opportunities and challenges associated with robots, autonomous systems and AI from technological, economic, socio-cultural, ethical and legal perspectives. The council is made up of an eight-member team of international and Austrian experts. In 2018, the council published its first white paper on Shaping the Future of Austria with Robotics and Artificial Intelligence. Information provided by: https://oecd.ai/dashboards/countries/Austria	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology*	No

	Overview	RBC Issues Covered	Reference to International Instruments
Brazil	In 2019, Brazil's Minister of Science, Technology, Innovations, and Communications announced the creation of eight AI laboratories throughout the country. One of these laboratories will focus on the frontiers of knowledge in AI with cyber security, joining efforts with the Brazilian Army. The other seven will be directed towards applied AI. In December, the MTIC opened a public consultation to define the National Strategy for AI. Information provided by: https://oecd.ai/dashboards/countries/Brazil	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	No
Council of Europe	In 2018, the Council of Europe published a paper titled "A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework" which takes an interdisciplinary approach to investigating the threats and harms associated with digital technology, and who bears responsibility for those threats and harms. Information provided by: https://rm.coe.int/draft-study-of-the-implications-of-advanced-digital-technologies-inclu/16808ef255	*Human Rights, Labour Rights, Consumer Interests, Science and Technology*	No
European Commission	The European Commission approach to AI and robotics deals with technological, ethical, legal and socio-economic aspects to boost EU's research and industrial capacity and to put AI at the service of European citizens and economy. The Commission is increasing its annual investments in AI by 70% under the research and innovation programme Horizon 2020. It will reach EUR 1.5 billion for the period 2018-2020. Information provided by: https://oecd.ai/dashboards/countries/EuropeanUnion	*Human Rights, Consumer Interests, Science and Technology Competition, Taxation*	No
Finland	Finland has an Artificial Intelligence Programme guided by a steering group that was appointed by Minister of Economic Affairs Mika Lintilä in 2017. The group published its first report in 2017 titled, "Finland's Age of Artificial Intelligence: Turning Finland into a leading country in the application of AI". The Steering Group published a second report 2018 titled, "Artificial Intelligence: Four Perspectives on the Economy, Employment, Knowledge and Ethics." Information provided by: https://oecd.ai/dashboards/countries/Finland	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	No
France	France's National Commission for Information Technology and Liberties (CNIL), hosted a series of ethical debates on AI by the Digital Republic Bill, dedicated to wider data and knowledge dissemination, equal rights for internet users, and fraternity through an inclusive digital society. The result of the debates was the paper, "How Can Humans Keep the Upper Hand? The ethical matters raised by algorithms and artificial intelligence" published in December 2017. Information provided by: https://www.cnil.fr/en	*Disclosure, Human Rights, Consumer Interests, Science and Technology, Competition*	No
France and Canada	The Global Partnership on AI (GPAI) is an international and multi-stakeholder initiative that advances cutting-edge research and pilot projects on AI priorities to advance the responsible development and use of AI that respects human rights and shared democratic values, as elaborated in the OECD's Recommendation on AI. The Partnership was conceived by Canada and France during their G7 presidencies and at its launch on June 15, 2020 counted 13 other founding members: Australia, the European Union, Germany, India, Italy, Japan, Korea, Mexico, New Zealand, Singapore, Slovenia, the United Kingdom and the United States. With its Secretariat hosted at the OECD, the GPAI will bring together experts from industry, government, civil society, and academia. GPAI's mission is to "support the development and use of AI based on human rights, inclusion, diversity, innovation,	*Human Rights, Science and Technology, Competition*	No

	Overview	RBC Issues Covered	Reference to International Instruments
	and economic growth, while seeking to address the United Nations Sustainable Development Goals". Two Centres of Expertise (in Montréal, the International Centre of Expertise in Montréal for the Advancement of Artificial Intelligence (ICEMAI) and in Paris, the National Institute for Research in Digital Science and Technology (INRIA)) support the operation of four expert working groups on: Responsible AI (Montreal); Data Governance (Montréal); the Future of Work (Paris); and Innovation & Commercialisation (Paris). Information provided by: https://oecd.ai/wonk and https://oecd.ai/wonk/oecd-and-g7-artificial-intelligence-initiatives-side-by-side-for-responsible-ai		
Mexico	In 2018, the Mexican government and the National Digital Strategy Office supported a white paper titled "Towards an AI Strategy in Mexico: Harnessing the AI Revolution". The report highlights the potential social applications of AI to improve services for the lowest earning 80% of Mexicans, but it also predicts that 19% of all jobs in Mexico will be affected by automation over the next two years and that governments will need to respond to possible social disruption. The report provides 21 recommendations. Information provided by: https://oecd.ai/dashboards/countries/Mexico	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition, Taxation*	No
United Kingdom	In September 2016, the House of Commons Science and Technology Committee published a 44-page report on "Robotics and artificial intelligence." Information provided by: https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14506.htm https://futureoflife.org/ai-policy-united-kingdom/	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	No
STRATEGY			
Argentina	Argentina has proposed a plan for an AI ecosystem in the country that anticipates some of the risks AI could pose, especially in ethics and data protection. The policy covers the decade from 2020 to 2030 and falls under the Innovative Argentina 2030 Plan and the 2030 Digital Agenda. Information provided by: https://oecd.ai/dashboards/countries/Argentina and https://www.bnamericas.com/en/news/argentina-advances-national-ai-plan	*Disclosure, Human Rights, Labour Rights Environment, Consumer Interests, Science and Technology, Competition*	*No*
Australia	In 2018 Australia's Victorian All-Party Parliamentary Group on Artificial Intelligence published its Digital Economy strategy for developing Australia's digital services. The federal government has earmarked $29.9 million over four years to enhance Australia's efforts in AI and machine learning in the country's 2018-19 budget providing for the development of a national AI Ethics Framework. Information provided by: https://oecd.ai/dashboards/countries/Australia	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition, Taxation*	*No*
	In 2018, the Australia Human Rights Commission launched a project to directly address the human rights impact of AI and emerging technologies, which includes a robust engagement of international human rights law and may serve as a guide for other countries, available here: https://www.humanrights.gov.au/sites/default/files/document/publication/AHRC-Human-Rights-Tech-IP.pdf	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology*	*UNGPs*

	Overview	RBC Issues Covered	Reference to International Instruments
Brazil	Brazil has already supported the OECD AI Recommendation, which includes a set of five principles and five recommendations to governments. Information provided by: https://oecd.ai/dashboards/countries/Brazil	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*OECD*
Canada	In 2017, Canada appointed the Canadian Institute for Advanced Research (CIFAR) to develop and lead a $125 million Pan-Canadian Artificial Intelligence Strategy. The strategy objectives are: to increase the number of outstanding AI researchers and skilled graduates in Canada; to establish interconnected nodes of scientific excellence in Canada's three major centres for AI in Edmonton, Montréal and Toronto; to develop global thought leadership on the economic, ethical, policy and legal implications of advances in AI; and, to support a national research community on AI. Information provided by: https://oecd.ai/dashboards/countries/Canada	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
China	The New Generation of Artificial Intelligence Development Plan is headed by the Ministry of Science and Technology (MOST) and the AI Plan Promotion Office, driven by government-led subsidies. An AI Strategy Advisory Committee was established in November 2017 to conduct research on strategic issues related to AI and to make recommendations. China's AI Industry Development Alliance is co-sponsored by more than 200 enterprises and agencies nationwide and focuses on building a public service platform for the development of China's AI industry with which to integrate resources and accelerate growth. Information provided by: https://oecd.ai/dashboards/countries/Chinahttps://futureoflife.org/ai-policy-china/	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*
Czech Republic	In 2018, the Czech Republic has committed itself to support AI development in the academic, public and private sectors, mutual cooperation and international engagement. The National AI Strategy follows up on and meets the objectives of the Government Innovation Strategy 2019–2030 and is linked to the Digital Czech Republic programme. It was inspired by similar foreign strategic documents concerning AI and the support for the digitization of the industry and services. The strategy was prepared by the deputy Prime Minister, in close cooperation with the Ministry of Industry and Trade, and with public, private and research institutions, the general public and with the involvement of social partners. *https://www.mpo.cz/assets/en/guidepost/for-the-media/press-releases/2019/5/NAIS_eng_web.pdf*	*Human Rights, Consumer interests, Labour rights, Science and Technology*	
Denmark	In 2018, the Danish Government launched the "Strategy for Denmark's Digital Growth," which includes a focus on AI. The strategy allocates 1 billion DKK for initiatives running to 2025 and is based on recommendations from a Digital Growth Panel and the Danish Government's Disruption Committee. In 2017, Denmark published, "Towards a Digital Growth Strategy – MADE," highlighting the Danish centre for artificial intelligence (DCKAI). Denmark also has a Digital Strategy for 2016-2020, "A Stronger and More Secure Digital Denmark" published in 2016, that briefly mentions AI. Information provided by: https://oecd.ai/dashboards/countries/DenmarkInformation provided by: https://futureoflife.org/ai-policy-Denmark/	*Human Rights Labour Rights Consumer Interests Science and Technology, Competition, Taxation*	*No*
France	President Macron presented his strategy to make France a leader in AI at the Collège de France on 29 March 2018. That year the #FranceIA Strategy launched, focused on developing: a quality training offer and attracting top researchers; dynamic ecosystems of innovation encompassing French Tech start-ups and major industrial groups; and a favourable legislative and regulatory framework with the Law for a Digital Republic. Information provided by:	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*

	Overview	RBC Issues Covered	Reference to International Instruments
	https://oecd.ai/dashboards/countries/FranceInformation provided by: https://futureoflife.org/ai-policy-France/		
G20	In 2019, the G20 Trade Ministers and Digital Economy Ministers and released a Ministerial Statement on Trade and Digital Economy which covers Human-centered Future Society, Data Free Flow with Trust, Human-centered Artificial Intelligence, Governance Innovation, Security in the Digital Economy, SDGs and Inclusion and Trade agreements. In the annex, the G20 released AI Principles for Responsible Stewardship of Trustworthy AI. Information provided by: https://www.mofa.go.jp/files/000486596.pdf	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition, Taxation*	*OECD*
G7	In 2019, the G7 leaders commit to the Biarritz Strategy for an Open, Free and Secure Digital Transformation which led to the launch of the Global Partnership on AI (GPAI) in June 2020. Information provided by: https://futureoflife.org/Charlevoix-common-vision-future-artificial-intelligence/https://www.oecd.org/about/secretary-general/artificial-intelligence-g7-summit-france-august-2019.htm and https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition, Taxation*	*OECD*
Germany	In 2018, Germany adopted a national AI strategy based on the Federal Cabinet's Key Points for a Strategy on Artificial Intelligence, which was developed by the Federal Ministry of Education and Research, the Federal Ministry for Economic Affairs and Energy, and the Federal Ministry of Labour. Information provided by: https://oecd.ai/dashboards/countries/Germany and Social Affairs. https://futureoflife.org/ai-policy-germany/	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*
Hungary	In 2019, Hungary launched an AI Action plan to "define and form the institutional framework of the Hungarian data market and the AI ecosystem. In May 2020, Hungary's Artificial Intelligence Strategy 2020-2030 was adopted: https://digitalisjoletprogram.hu/files/6f/3b/6f3b96c7604fd36e436a96a3a01e0b05.pdf Information also provided by: https://oecd.ai/dashboards/countries/Hungary and https://www.cms-lawnow.com/ealerts/2019/10/hungary-announces-ai-action-plan	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*
India	In 2018, India defined a national policy on AI in a working paper titled, "National Strategy for Artificial Intelligence #AIforAll." The paper includes a section on "Ethics, Privacy, Security, and Artificial Intelligence".. Information provided by: https://oecd.ai/dashboards/countries/India and https://www.ceps.eu/system/files/RR%20No2018-09_Germany%27s%20NetzDG.pdf https://futureoflife.org/ai-policy-india/#:~:text=In%20June%202018%2C%20the%20Indian,agriculture%2C%20education%2C%20urban%2D%2Fsmart	*Disclosure, Human Rights, Labour Rights, Environment, Consumer, Interests, Science and Technology, Competition*	*No*
Ireland	In 2018, the Irish Economic Development Agency (IDA) and Enterprise Ireland created an infographic highlighting Ireland's strengths in AI and characterizing Ireland's strategy as the "AI Island". To develop this, they audited the country's AI ecosystems and organized a collaborative workshop in 2017 involving industry, government and academia. Information provided by: https://www.idaireland.com/newsroom/publications/artificial-intelligenceInformation provided by:	*Science and Technology, Competition, Taxation*	*No*

	Overview	RBC Issues Covered	Reference to International Instruments
Japan	In 2017, Japan released an "Artificial Intelligence Technology Strategy", focusing on promoting AI development and determining phases and priorities for industrialization including productivity, healthcare, and mobility. Information provided by: https://oecd.ai/dashboards/countries/Japan	*Disclosure, Consumer Interests, Science and Technology, Competition, Taxation*	*No*
Lithuania	In 2019, Lithuania published the Lithuanian Artificial Intelligence Strategy: A Vision of the Future. The report includes recommendations to the government with the goal to "modernize and expand the current AI ecosystem in Lithuania and ensure that the nation is ready for a future with AI." The report recommends establishing an AI Ethics committee, involving representatives from academia, government, industry and NGOs. Information provided by: https://oecd.ai/dashboards/countries/Lithuaniahttps://futureoflife.org/ai-policy-Lithuania/	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*
Nordic-Baltic Region	Ministers from Denmark, Estonia, Finland, the Faroe Islands, Iceland, Latvia, Lithuania Norway, Sweden, and the Åland Islands issued a declaration of collaboration on AI in 2018, "AI in the Nordic-Baltic region." The countries aim to collaborate on skill development, data access, standards and principles, ensuring the role of AI in the European Digital Single Market, avoiding unnecessary regulation, and utilizing the Nordic Council of Ministers to facilitate collaborate. Information provided by: https://oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-24254Information provided by:	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition*	*No*
Russian Federation	In 2019, Russia released a national AI strategy, Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation. Information provided by: https://oecd.ai/dashboards/countries/RussianFederationhttps://futureoflife.org/ai-policy-Russia/	*Disclosure, Human Rights, Labour Rights, Bribery, Consumer Interests, Science and Technology, Competition*	*No*
Singapore	In 2019, Singapore launched a National AI Strategy, considering AI alongside the Internet of Things, cloud computing, big data analysis, and mobile technologies. The strategy identifies five national AI projects including transport and logistics, smart cities and estates, healthcare, education, and safety and security. Information provided by: https://oecd.ai/dashboards/countries/Singapore	*Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
Korea	In 2016, South Korea launched its "Realizing a Human-Centred Intelligent Information Society" strategy for engaging businesses, citizens, government and the research community. The strategy focuses on public concerns of loss of jobs, and unsafe/inappropriate use of technologies and on businesses' concerns of having a shortage of experts, excessive regulation, and the lack of an industrial ecosystem and infrastructure. Information provided by: https://oecd.ai/dashboards/countries/SouthKorea	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition, Taxation*	*No*
Spain	In 2019, Spain's Ministry of Science, Innovation and Universities released an R&D Strategy in Artificial Intelligence. The report was authored by the General Secretariat of Scientific Policy Coordination within the Ministry as well as by the Artificial Intelligence Task Force and called for the development of a National AI Strategy which is currently in development. Information provided by: https://oecd.ai/dashboards/countries/SpainInformation provided by: https://futureoflife.org/ai-policy-Spain/	*Human Rights, Labour Rights, Environment, Science and Technology, Competition*	*No*
Sweden	In 2018 Sweden released its "National Approach for Artificial Intelligence," guiding document outlining what the country needs to be at the forefront of AI development and use. Information provided by: https://oecd.ai/dashboards/countries/Sweden	*Human Rights Science and Technology, Competition*	*No*

	Overview	RBC Issues Covered	Reference to International Instruments
Switzerland	On 18 October 2018, Federal Councillor Johann N. Schneider-Ammann, together with the umbrella organisations of the Swiss social partners and in the presence of the Director-General of the International Labour Organisation (ILO) Guy Ryder, signed a tripartite declaration on the future of work and social partnership in Switzerland in the age of economic digitisation.	*Labour Rights, Science and Technology*	*ILO*
United Arab Emirates	In 2017, the UAE announced its Strategy for Artificial Intelligence, which was approved in 2019. The policy aims to achieve the objectives of UAE Centennial 2071; boost government performance at all levels; use an integrated smart digital system that can overcome challenges and provide quick efficient solutions; make the UAE the first in the field of AI investments in various sectors; and create new vital market with high economic value. Information provided by: https://oecd.ai/dashboards/countries/UnitedArabEmirates	*Human Rights, Labour Rights, Environment, Science and Technology, Competition*	*No*
United Kingdom	The UK's Sector deal on AI in 2019 reinforced the 5 foundations of the Industrial Strategy (Ideas, People Infrastructure, Business Environment and Places) and draws on the government's Digital Strategy which focuses on strengthening telecoms, data and enterprise. Information provided by: https://oecd.ai/dashboards/countries/UnitedKingdom and https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal	*Human Rights, Labour Rights, Science and Technology, Competition*	*No*
United States of America	As of 2019, President Trump's American AI Initiative as of 2019 includes : AI for American Innovation for R&D by the Select Committee on AI under the National Science and Technology Council; AI for American Industry: Transportation, Healthcare, Manufacturing, Financial Services, Agriculture, Weather Forecasting, and National Security and Defense; AI for the American Worker including an executive order charging companies and trade groups across the country to sign a pledge committing to expand education, training, and reskilling opportunities for American workers among other educational initiatives; and AI with American Values. Information provided by: https://oecd.ai/dashboards/countries/UnitedStateshttps://futureoflife.org/ai-policy-united-states/ and https://www.whitehouse.gov/ai/	*Disclosure, Human Rights, Labour Rights, Consumer Interests, Science and Technology, Competition, Taxation*	*OECD*

Social media initiatives by country/territory/organisation/region

	Overview	RBC Issues Covered	International Instruments
LEGISLATION			
Angola	In 2019, Angola approved a new penal code pertaining specifically to crimes committed in the media. These include fines and up to six months' imprisonment for "abuse of press freedom," a charge that can be drawn by speech deemed as inciting crimes, disseminating hate speech, or defending fascist or racist ideologies. The measure also covers those who disseminate texts, images, or sounds obtained by fraudulent means, as well as those who intentionally publish fake news. Information provided by: https://freedomhouse.org/report/freedom-net/2019/angola	*Disclosure, Human Rights, Consumer Interests*	*No*
Australia	In 2019, Australia published a bill called the Sharing of Abhorrent Violent Material amendment, criminalizing "abhorrent violent material," which it defines as videos that show terrorist attacks, murders, rape or kidnapping. Social media companies that fail to remove such content "expeditiously" could face fines of up to 10% of their annual profit, and employees could be sentenced to up to three years in prison. Companies must also inform the police when illegal material is found.	*Disclosure, Human Rights, Consumer Interests, Taxation*	*No*
Bangladesh	In 2019, Bangladesh's Digital Security Act (DSA replaced the controversial section 57 of the Information and Communication Technology Act (ICT Act). It grants law enforcement authorities wide-ranging powers to remove or block online information that "harms the unity of the country or any part of it, economic activities, security, defense, religious values or public order or spreads communal hostility and hatred." The government announced a new social media monitoring program to identify "fake news" and propaganda online for enforcement. Information provided by: https://www.hrw.org/news/2018/10/19/bangladesh-crackdown-social-media	*Disclosure, Human Rights, Consumer Interests*	*No*
Belarus	In 2018, New amendments to Belarus's Mass Media law expanded the Ministry of Information's ability to block and filter content, empowering it to suspend, block, and close registered and unregistered online outlets without warning or judicial oversight. These amendments empower the ministry to block social media platforms, and to hold website owners liable for hosting content deemed false, defamatory, or harmful to the national interest. Owners can also be liable for comments by unidentified persons posted to their sites. Information provided by: https://www.freedomonthenet.org/country/belarus/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Brazil	Preceding Brazil's 2018 general elections, several draft bills were proposed to criminalize the dissemination of false news. Proposed penalties ranged from small fines to up to eight years of imprisonment. While they were archived at the end of 2018, some of these proposals were relaunched and continued to be discussed. Information provided by: https://www.freedomonthenet.org/country/brazil/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
China	In 2015, new legislation introduced penalties of up to seven years in prison for the dissemination of misinformation on social media. https://www.freedomonthenet.org/country/china/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
	In 2015, the antiterrorism law instructed companies to delete terrorist content or face administrative detention for their personnel. It barred social media users from sharing information about acts of terrorism or spreading "inhuman" images that could encourage copycat attacks, and increased pressure on private companies to provide the government with user data. Information provided by: https://www.freedomonthenet.org/country/china/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Egypt	In 2018, President Sisi signed a new law that compels media outlets to obtain a license from the Supreme Council for Media	*Disclosure, Human Rights,*	*No*

	Overview	RBC Issues Covered	International Instruments
	Regulation. The legislation defines media outlets to include any website or social media account with at least 5,000 subscribers, and the individuals behind such outlets could be subject to account deletion, fines, and imprisonment if they are found to be spreading false news. Information provided by: https://www.freedomonthenet.org/country/Egypt/freedom-on-the-net/2019	*Consumer Interests, Taxation*	
EU	The EU's General Data Protection Regulation (GDPR), enforced in 2018, establishes new protections for European citizens' rights around data protection and privacy, which impacts any organization collecting European residents' data. Information provided by: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en	*Disclosure, Human Rights, Consumer Interests, Science and Technology, Taxation*	*No*
France	In 2018, Parliament passed a law that aims to combat disinformation around elections by empowering judges to order the removal of "fake news" within three months of an election. Judges have 48 hours to decide whether a website is spreading fake news following a referral by a public prosecutor, political party, or interested individual. Under the law, social media platforms are also required to disclose who is paying for sponsored ads during electoral campaigns. Information provided by: https://www.freedomonthenet.org/country/France/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Germany	Germany's Network Enforcement Act, or NetzDG law serves to combat hate speech on the internet. Under the 2018 law, online platforms face fines of up to €50 million for systemic failure to delete illegal content. Companies with more than 2 million registered users in Germany are required to establish an effective and transparent procedure to receive and review complaints of allegedly illegal content. They must block or remove "manifestly unlawful" content within 24 hours of receiving a complaint but have up to one week or potentially more if further investigation is required. In especially complex cases, companies can refer the case to an industry-funded but government-authorized body that is required to make determinations within a seven-day window. The government has authorized the FSM Freiwillige Selbstkontrolle Multimedia-Diensteanbieter as such a body in January 2020. (https://www.fsm.de/en/netzdg).	*Disclosure, Human Right, Science and Technology, Taxation*	*No*
Jordan	In 2017, Jordan's government proposed a series of controversial new amendments to the Cybercrime Law to explicitly cover hate speech, defined as "any statement or act that would incite discord, religious, sectarian, ethnic or regional strife or discrimination between individuals or groups. The bill also criminalises spreading rumours and false news, without providing a clear definition of the offenses, with up to two years in prison and a fine. In February 2019, the lower house of Parliament rejected the bill, however, the legislation was being considered by the Senate as of April 2019. Information provided by: https://www.freedomonthenet.org/country/Jordan/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Kazakhstan	According to Kazakhstan's 2016 Mass Media Law web publishers—including bloggers and social media users— are liable for the content they post. In 2015, the Ministry of Information and Communication stated that social media users could be held liable for extremist comments posted on their pages by third parties, as permitting the publication of extremist materials in a mass media outlet is an offense under the criminal code that can be punished with up to 90 days in jail. In 2016, the Ministry of Information and Communication gained the authority to issue takedown and blocking orders until website owners remove specific content. Information provided by: https://www.freedomonthenet.org/country/kazakhstan/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Kenya	The 2018 Computer Misuse and Cybercrimes law in Kenya punishes the spreading of "false information" and imposes a lengthy jail term on offenders. It proposes a fine of $50,000 and/or up to two years in prison for publishing "false" information. The law also criminalizes abuse on social media and cyber bullying. Information provided by: https://www.bbc.com/news/world-africa-44137769	*Disclosure, Human Rights, Consumer Interests*	*No*

	Overview	RBC Issues Covered	International Instruments
Malaysia	Malaysia passed the Anti-Fake News Bill in 2018, weeks before the country held national elections. The law cites the following offences: Creating, offering, publishing etc. fake news or publications containing fake news; providing financial assistance for purposes of committing or facilitating commission these offences; failing to carry out the duty to remove fake news. The law permits courts to mandate the removal of publications containing fake news or authorize the removal of fake news by a police officer or authorized officer under the Communications and Multimedia Act (1998) Information provided by: https://www.accessnow.org/malaysias-dangerous-fake-news-law-is-still-on-the-books-it-must-be-repealed/ and https://www.cljlaw.com/files/bills/pdf/2018/MY_FS_BIL_2018_06.pdf	*Disclosure, Human Rights, Consumer Interests*	*No*
Russian Federation	In 2019, President Putin signed a set of bills that make it a crime to "disrespect" the state and spread "fake news" online; Users that spread "fake news" will face fines of up to 1.5 million rubles for repeat offenses. As is the case with other Russian laws, the fines are calculated based on whether the offender is a citizen, and any official or a legal entity that spreads "fake news" will face fines of up to 1.5 million rubles for repeat offenses. Insulting state symbols and the authorities, including Putin, will carry a fine of up to 300,000 rubles and 15 days in jail for repeat offenses. Information provided by: https://www.themoscowtimes.com/2019/03/18/putin-signs-fake-news-internet-insults-bills-into-law-a64850	*Disclosure, Human Rights, Consumer Interests, Taxation*	*No*
Rwanda	Rwanda's cybersecurity law of 2018 imposes up to five years imprisonment and a fine between 1 million francs and 3 million francs for publishing "rumours that may incite fear, insurrection or violence…or that may make a person lose their credibility." Anyone who "establishes, publishes, or uses a site of a terrorist group" faces imprisonment of 15 to 20 years and a fine between 20 million and 50 million francs. Notably, the spread of "false information or harmful propaganda with intent to cause a hostile international opinion against [the] Rwanda government" carries penalties of between seven and ten years in prison in peacetime and life imprisonment during wartime. Information provided by: https://www.freedomonthenet.org/country/rwanda/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Singapore	Singapore's protection from Online Falsehoods and Manipulation Bill (2019) is intended to "prevent the electronic communication of false statements of fact" by imposing harsh penalties. Individuals who do not publish corrections or comply with takedown requests can be subjected to 12 months in prison or fines of up to S$20,000. ISPs that do not carry out blocking orders can also be fined up to S$20,000 a day, with an upper limit of S$500,000. Websites with three published falsehoods within 6 months can have advertising money restricted. The use of bots or an "inauthentic online account" to communicate false content mandates a prison term of up to 10 years and fines of up to S$100,000. Information provided by: https://www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-online-falsehoods-and-manipulation-bill10-2019.pdf and https://freedomhouse.org/blog/citing-fake-news-singapore-could-be-next-quash-free-expression	*Disclosure, Human Rights, Consumer Interests*	*No*
Sudan	Amendments in 2019 to the Media Law imposed restrictions on online journalism and social media, including requiring online journalists to register with the Journalism Council, which has the power to suspend publications and prevent online journalists from posting content it objects to. In June 2018, the National Assembly passed the Law on Combating Cybercrimes of 2018, which introduced criminal penalties for the spread of fake news online. Information provided by: https://www.freedomonthenet.org/country/sudan/freedom-on-the-net/2019#C2	*Disclosure, Human Rights, Consumer Interests*	*No*
Tech Against Terrorism	In the aftermath of the 2017 terror attack in Christchurch, New Zealand, government leaders and online platforms agreed on the Christchurch Call for Action. In response, the EU Internet Forum produced the EU Protocol to allow Member States and online platforms to respond rapidly and in a coordinated manner to the dissemination of terrorist content online in the event of a terrorist attack.	*Human Rights, Consumer Interests, Science and Technology*	*No*

	Overview	RBC Issues Covered	International Instruments
United Kingdom	The Counter-Terrorism Internet Referral Unit (CTIRU) was set up in 2010 by ACPO (and run by the Metropolitan Police) to remove unlawful terrorist material content from the Internet with a focus on UK based material. CTIRU works with internet platforms to identify content which breaches their terms of service and requests that they remove the content on a voluntary basis. CTIRU also compiles a list of URLs for material hosted outside the UK which are blocked on networks of the public estate. Information provided by: https://www.counterterrorism.police.uk/together-were-tackling-online-terrorism/	*Human Rights, Consumer Interests*	*No*
California (United States of America)	California Consumer Privacy Act (CCPA) enacted in 2018, creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. Businesses are subject to the CCPA if one or more of the following are true: Has gross annual revenues in excess of $25 million; buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices; derives 50 percent or more of annual revenues from selling consumers' personal information. As proposed by the draft regulations, businesses that handle the personal information of more than 4 million consumers will have additional obligations. Information provided by: https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf	*Disclosure, Human Rights, Consumer Interests, Taxation*	*No*
Viet Nam	The cybersecurity law of 2019 prohibits a wide range of activities conducted online, including organizing opposition to the CPV; distorting Vietnam's revolutionary history and achievements; spreading false information; and harming socioeconomic activities. In addition, websites and individual social media pages are prohibited from posting content critical of the state or that causes public disorder. Information provided by: https://www.freedomonthenet.org/country/vietnam/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Zambia	In 2018, the cabinet approved review of the draft on Cybersecurity and Cybercrimes Bill. In particular, the draft bill provides penalties of up to one year in prison, fines, or both for "any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person." The legislation has not been made available for public scrutiny and has not been debated in the parliament. Information provided by: https://www.freedomonthenet.org/country/zambia/freedom-on-the-net/2019#C2	*Disclosure, Human Rights, Consumer Interests*	*No*
Zimbabwe	In Zimbabwe, the government is considering a draft law that would criminalise certain forms of online speech and activity. The draft was approved by the cabinet in October 2019, though it has yet to make its way through Parliament. The Cyber Crime Bill draft penalises the dissemination of communications "with intent to coerce, intimidate, harass, threaten bully or cause substantial emotional distress" with a fine, prison terms of up to 10 years, or both, and penalises the spread of false information "to cause psychological or economic harm" with fines, up to five years in prison, or both. Information provided by: https://www.freedomonthenet.org/country/Zimbabwe/freedom-on-the-net/2019#B	*Disclosure, Human Rights*	*No*
RECOMMENDATIONS			
Global Counter-terrorism Forum	Co-chaired by Australia and Indonesia, the Countering Violent Extremism (CVE) Working Group focuses on diminishing radicalization and recruitment to terrorism through internationally, regionally, nationally and locally owned and relevant approaches to CVE. In September 2018, Australia, Switzerland and the United Kingdom launched an Initiative to develop a Policy Toolkit to operationalize the Zurich-London Recommendations. The Toolkit provides a practical and user-friendly guide for policymakers and governmental experts on good governmental practices, case studies, and references to existing international and regional initiatives and practices in preventing and countering violent extremism and terrorism online. Information provided by:	*Disclosure, Human Rights, Consumer Interests, Science and Technology*	*No*

	Overview	RBC Issues Covered	International Instruments
	https://www.thegctf.org		
United Kingdom	The Online Harms White Paper (2019) sets out the UK Government's plans to make companies more responsible for their users' safety online, especially children, and will help to build trust in digital markets. The White Paper outlines the government's intention to establish in law a new 'duty of care' on companies towards users. The 'duty of care' will ensure companies have appropriate systems and processes in place to deal with harmful content on their services to keep their users safe. An initial response to the Online Harms White Paper consultation was published in February 2020. Information provided by: https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#executive-summary https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response	*Disclosure, Human Rights, Consumer Interests, Science and Technology*	*No*
STRATEGY			
EU	Established in 2015, the EU Internet Referral Unit (EU IRU) detects and investigates malicious content on the internet and in Social Media. The work of the EU IRU, which is based at Europol's European Counter Terrorism Centre, not only produces strategic insights into terrorism, but also provides information for use in criminal investigations. On average, the content flagged for referrals has been removed in 86% of the cases (Figures of December 2017). Information provided by: https://www.europol.europa.eu/about-Europol/EU-internet-referral-unit-EU-ire	*Disclosure, Human Rights Science and Technology*	*No*
Italy	Leading up to the March 2018 elections, the Italian government announced the launch of an online portal to report "fake news" to the postal police. Project "red button," gives citizens the opportunity to report fake news using a portal on the police's website. The National Anti-Crime Information Centre for Critical Infrastructure Protection was tasked with analysing the reported content. According to the plan, the police website and their social media accounts would be set to publish retractions, based on their analysis of reported content. Information provided by: https://freedomhouse.org/report/freedom-net/2018/italy	*Human Rights, Consumer Interests, Science and Technology*	*No*
Jordan	Jordan's Aqaba Process is a multi-national forum led by His Majesty King Abdullah II to enhance global coordination in the fight against terrorism and violent extremism. The 2015 session of the Aqaba Process, included heads of state, government officials and law enforcement officials from throughout the region, Europe and Africa, focused on combatting terrorism in East Africa and developing approaches to countering emerging security challenges.	*Disclosure, Human Rights, Consumer Interests, Science and Technology*	*No*
Malaysia	The Barisan Nasional Government (in place until May 2018), took steps to combat what it characterized as "false news" in 2017. Sebernarnya, a fact-checking portal launched by the Communications and Multimedia Ministry, encouraged social media users to verify the content of all news reports shared on popular platforms with the slogan, "not sure, don't share." Officials said the portal was nonpartisan, and the following government retained it. Information provided by: https://www.freedomonthenet.org/country/malaysia/freedom-on-the-net/2019	*Disclosure, Human Rights, Consumer Interests*	*No*
Thailand	In 2019, Digital Economy and Society Minister Puttipong Punnakanta announced an initiative to establish a Fake News Centre, whose mission would be to combat false and misleading information on social media that jeopardizes people's safety or violates the CCA.On November 1st 2019, Reuters reported that the Centre had been established. Information provided by: https://www.freedomonthenet.org/country/thailand/freedom-on-the-net/2019#C2;and https://www.reuters.com/article/us-thailand-	*Human Rights, Consumer Interests*	*No*

	Overview	RBC Issues Covered	International Instruments
	fakenews/thailand-unveils-anti-fake-news-center-to-police-the-internet-idUSKBN1XB48O		

Artificial intelligence initiatives by civil society organisations

Organisation	Overview	RBC Issues Covered	International Instruments
BEST PRACTICE GUIDANCE			
Access Now	In 2018, Access Now published a report on the potential range of human rights issues that may be raised by emerging AI technologies through the lens of human rights law. Access Now points out that "many of the issues that arise in examinations of [AI] are not new, but they are greatly exacerbated by the scale, proliferation, and real-life impact that artificial intelligence facilitates." The paper gives recommendations on how to address human rights harms. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*Refers to Human Rights (HR, hereafter)*
AI Now Report	AI Now released a report in 2017 as a result of the AI Now symposium (2016 and 2017) and in conjunction with the Obama White House's Office of Science and Technology Policy and the National Economic Council. The report advocates for "the immediate need to understand AI technologies in the context of existing social systems, to connect technological development to social and political concerns, to develop ethical codes with force and accountability, to diversify the field of AI and to integrate diverse social scientific and humanistic research practices into the core of AI development. https://ainowinstitute.org/AI_Now_2017_Report.pdf	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
Amnesty International and AccessNow	The Toronto Declaration by Amnesty International and AccessNow (2018) focuses on protecting the right to equality and non-discrimination in machine learning systems according to internationally recognized human rights and standards. The report first applies the framework of human rights law, addressing the right to equality and non-discrimination and promoting diversity and inclusion. Next, the report outlines the duties of States when using ML systems, promoting equality and accountability by the private sector. The report tasks the private sector with human rights due diligence and fulfilling the right to effective remedy. https://www.amnesty.org/en/documents/pol30/8447/2018/en/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*UNGP*
FAT/ML	FAT/ML's 2016 "Principles for Accountable Algorithms and a Social Impact Statement for Algorithms" is designed for developers and product managers to implement algorithmic systems in publicly accountable ways. Accountability in this context includes an obligation to report, explain, or justify algorithmic decision-making as well as mitigate any negative social impacts or potential harms. FAT/ML recommends that companies publicly commit to associated best practice by having algorithm creators develop a Social Impact Statement using their principles as a guiding structure. FAT/ML recommends that the statement be revisited and reassessed (at least) three times during the design and development process and, when the system is launched, made public as a form of transparency so that the public has expectations for social impact of the system.https://www.fatml.org/resources/principles-for-accountable-algorithms	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
Data and Society	"Governing Artificial Intelligence: "Upholding Human Rights and Dignity and provides a snapshot of stakeholder engagement at the intersection of AI and human rights. The paper breaks down stakeholder initiatives by AI and human rights activity in business, civil society, governments, the UN, intergovernmental organizations, and academia. Recommendations include: Developing effective	*Disclosure, Human Rights, Labour Rights, Environment, Consumer*	*OECD, UNGP*

Organisation	Overview	RBC Issues Covered	International Instruments
	channels of communication between technology companies and local civil society groups; technology companies and researchers conducting HR-IAs throughout the life cycle of their AI systems; Governments developing national AI policies, guidelines, and possible regulations; cross-sector collaboration on the development of operationalization of human rights in business; and continuing the research and publication of the human rights impacts resulting from AI systems by UN human rights investigators and special rapporteurs.https://datasociety.net/library/governing-artificial-intelligence/	*Interests, Science and Technology, Competition*	
UNI Global Union	UNI Global Union represents 20 million workers from over 150 countries in the services sector. In 2017 the UNI released "Top 10 Principles for Workers' Data Privacy and Protection" to address a gap between companies' increasing use of data, big data and data sets, and workers' data protection and privacy rules. The paper addresses data provided by workers such as CVs, fingerprints or iris scans, data mined on workers by employers to monitor workflow, and data use by management in hiring, promotions, and discipline. The paper advocates for workers' and union representatives' right to access, influence, edit and delete data that is collected on them and via their work processes. Notably, the UNI recommends a multi-disciplinary inter-company data governance body should be established to govern data formation, storage, handling and security issues and integrating all its proposed principles through sectoral collective bargaining. http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*UDHR*
Association for Computing Agency Professional Ethics in Computing	The latest version of the Association for Computing Agency (ACM) Code of Ethics and Professional Conduct ("the Code") is the 2018 version, which was adopted by the ACM Council on June 22, 2018. Before this, the Code was most recently updated in 1992; changes in the nature of computing's impact (including with the emergence of AI systems) means that every decision requires computing professionals to identify a broader range of stakeholders and consider how to satisfy our obligations to them. A primary function of the Code is to help computing professionals identify potential impacts and promote positive outcomes in their systems. https://www.acm.org/code-of-ethics	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
World Economic Forum	The World Economic Forum's Whitepaper "A Framework for Developing a National Intelligence Strategy" (2019) makes the case for why states need national AI strategies, and how to design those strategies. One of the paper's key points is that AI raises unprecedented challenges for governments in relation to algorithmic accountability, data protection, explainability of decision-making by machine-learning models and potential job displacements. The proposed AI framework is the result of a holistic study of the various strategies and national plans prepared by various countries, including Canada, the United Kingdom, the United States, India, France, Singapore, Germany and the UAE. Additionally, the World Economic Forum team has interviewed government employees responsible for developing their national AI strategies, in order to gain a detailed understanding of the design process they followed. https://www.weforum.org/whitepapers/a-framework-for-developing-a-national-artificial-intelligence-strategy	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
RATINGS AND RANKINGS			
Berkman Klein Center for Internet and Society at Harvard University	The Principled AI Project (January 2020) analysed the contents of thirty-six prominent AI principles which, in wording or in process, identified thematic trends that suggest the earliest emergence of sectoral norms. https://cyber.harvard.edu/publication/2020/principled-ai	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*Refers to HR*
Ranking Digital Rights	Ranking Digital Rights (RDR) works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights. RDR does this by ranking the world's most powerful internet, mobile, and telecommunications companies on relevant commitments and policies, based on international human rights standards.	*Disclosure, Human Rights, Labour Rights, Environment, Consumer*	*UNGPs*

Organisation	Overview	RBC Issues Covered	International Instruments
	https://rankingdigitalrights.org/index2019/	*Interests, Science and Technology, Competition*	
VOLUNTARY INITIATIVES			
Future of Life Institute	The Asilomar principles were developed in conjunction with the 2017 Asilomar conference. The principles address research issues, ethics and values, and long-term issues. Notably, the principles specify that an arms race in lethal autonomous weapons should be avoided. Furthermore, they recognise that AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity, must be subject to strict safety and control measures. https://www.oecd.org/going-digital/ai-intelligent-machines-smart-policies/conference-agenda/ai-intelligent-machines-smart-policies-oheigeartaigh.pdf	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*Refers to HR*

Social media initiatives by civil society organisations

Organisation	Overview	RBC Issues Covered	International Instruments
BEST PRACTICE GUIDANCE			
Santa Clara Principles on Content Moderation	Developed by civil society, the Santa Clara Principles outline minimum levels of transparency and accountability for platform companies which moderate content online. For example, companies should publish the numbers of posts removed, and accounts removed permanently or temporarily suspended due to violations of their content guidelines, and provide notice to each user whose content is taken down or whose account is suspended about the reason for the removal or suspension. https://santaclaraprinciples.org/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*

Artificial intelligence and social media initiatives by civil society organisations

Organisation	Overview	RBC Issues Covered	International Instruments
BEST PRACTICE GUIDANCE			
IEEE	In 2017 the IEEE published a Global Initiative on Ethics of Autonomous and Intelligent Systems released a report titled, "From Principles to Practice Ethically Aligned Design Conceptual Framework" providing general principles and ethical foundations, followed by a discussion of areas of impact, including: sustainable development, personal data rights and agency over digital	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology,*	*Refers to HR*

	identity, legal frameworks for accountability and policies for education and awareness. In the paper's section specifically on Social Media, the IEEE recommends increasing transparency and user control; using AI to detect untruthful information; requiring companies to provide algorithmic transparency and business transparency, clarifying legislation between "platforms" and "content providers" and promoting the right to information. https://standards.ieee.org/news/2017/ieee_global_initiative.html	*Competition*	

Multi-Stakeholder artificial intelligence initiatives

Organisation	Overview	RBC Issues Covered	International Instruments
BEST PRACTICE GUIDANCE			
Artificial Intelligence Network of Excellence in Sub-Saharan Africa	In 2019, the Network held a three-day workshop (Nairobi Workshop) which focused on three critical areas: Policy and regulations; skills and capacity building; and the application of AI in Africa. The 5-year target outcomes of the workshop include: A commitment by 30 African countries to have AI specific policies that include multi-stakeholder evidence-based inputs, and AI regulation that is ethics and rights based; a commitment to have 5 regional research centres and 500 researchers. The meeting gathered sixty African and international experts. https://ai4d.ai/event/ssa-network/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
C Minds	C-Minds is a women-led team that designs and deploys initiatives for social change with and from the Global South. The AI for Good Lab is where C Minds explores how to strengthen Mexico and the Latin American region in the face of the international AI and Tech Revolution, boosting the ecosystem, deepening ethical conversations and contributing more ethical, fair and inclusive AI policy. As a part of the AI for good lab with the IEEE, C Minds is founding and chairing the Latam Circle, part of the institute's AI ethics global initiative, working with 5 different countries to boost the region's participation in the creation of global AI standards. In 2018, the group published a paper titled "Towards an AI Strategy in Mexico: Harnessing the AI Revolution". Involved parties included: IDB, Microsoft, Tecnológico de Monterrey, and Open Data Institute. https://www.cminds.co/ai	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
Global Symposium on Artificial Intelligence and Inclusion	The Global Symposium on AI and Inclusion held in Brazil in 2017 sought to address issues that exist at the intersection of AI development and the application divide between the Global North and the Global South. Some of the thematic areas included health and wellbeing, education, and humanitarian crisis mitigation, as well as cross-cutting themes such as data and infrastructure, law and governance, and algorithms and design. Involved parties included: MIT Media Lab, Berkman Klein Center for Internet and Society at Harvard University, the Institute for Technology and Society Rio, and the Global Network of Internet and Society Research Centres, the Ethics and Governance of Artificial Intelligence Fund, International Development Research Centre (IDRC), the Open Society Foundations, and the Museum of Tomorrow. https://networkofcenters.net/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	No
OECD	The OECD principles on AI identify value-based principles for the stewardship of AI, including the benefit to society, rights respecting by design, transparency and responsible disclosure around AI systems; safety, and security, and accountability. The OECD provides recommendations to governments, on public and private investment in research and development, fostering accessible AI ecosystems, ensuring a policy environment that supports the deployment of	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	OECD

Organisation	Overview	RBC Issues Covered	International Instruments
	trustworthy AI systems, empowering people with the skills for AI and support workers for a fair transition and cooperating across borders and sectors to progress on responsible stewardship of trustworthy AI. OECD Members and Adherents: Argentina, Brazil, Colombia, Costa Rica, Malta, Peru, Romania and Ukraine. https://www.oecd.org/going-digital/ai/principles/		
RATINGS AND RANKINGS			
Future of Life Institute	The AI Policy Challenges and Recommendations of the Future of Life Institute include a review of 14 areas of concern for the safe and beneficial development of AI, both in the near future and in the long-term. The review serves as an educational resource for policymakers seeking to harness the benefits of AI while preparing for and mitigating potential threats. The topics are not sector-specific (i.e. transportation or healthcare), but address overarching AI policy concerns that cut across multiple industries. Benchmarked Groups: Future of Life Institute Similar AI Principles, G7, DeepMind Ethics and Society Principles, IEEE: Ethically Aligned AI Design, Google AI Principles, ITI AI Policy Principles, AI Now (2017) Report, British Standard guide to the ethical design and application of robots and robotic systems, The Toronto Declaration, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation" written by 26 Authors from 14 Different Institutions, Human Rights Watch, and the Campaign to Stop Killer Robots. https://futureoflife.org/ai-policy-challenges-and-recommendations/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
VOLUNTARY INITIATIVES			
AI for Good Global Summit	The AI for Good Global Summit (2019) is the leading UN platform for global and inclusive dialogue on AI. Building on the success of previous years, the 2019 AI for Good Global Summit continued to collaborate with AI innovators and other stakeholders, including more than 37 UN agencies and bodies, to identify strategies to ensure that AI technologies are developed in a trusted, safe and inclusive manner, with equitable access to their benefits. Involved groups: CTBTO, FAO, ICAO, ILO, IMO, IOM, UNAIDS, UNCTAD, UNDESA, UNDPPA (former UNDPA), UNECE, UNEP, UNESCO, UNFCCC, UNFPA, UNGP, UNHabitat, UNHCR, UNICEF, UNICRI, UNIDIR, UNIDO, UNDRR (former UNISDR), UNITAR, UNODA, UNODC, UNOOSA, UNOPS, UNRISD, UNU, UNWomen, UNWTO, WFP, WHO, WIPO, WMO and World Bank Group (WBG). https://aiforgood.itu.int/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*UNGPs*
IA2030Mx	The organization works to advance the use and application of AI to benefit Mexicans, strengthen coordination between sectors, deepen the debate about current and future AI opportunities, develop Mexican talent in AI, make Mexico a competitive and fair country, and make the knowledge of AI accessible to all people. IA2030Mx is a multi-sectoral coalition composed of professionals, academic institutions, companies, start-ups, public agencies and other key actors of the digital ecosystem and Artificial Intelligence (AI) in Mexico. Parties include: Amexcomp, Blue Messaging, C Minds, Coparmex, The British Embassy in Mexico, UDEM, Iniciativa en Inteligencia Artificial, and AI Mexico. www.IA2030Mx.mx	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*OECD*
Partnership on AI	The Partnership on AI (PAI) has 8 tenets, primarily focusing on stakeholder engagement and dialogue seeking to maximize the potential benefits of AI for as many people as possible. The Partnership was formally established in late 2016, led by a group of AI researchers representing six of the world's largest technology companies: Apple, Amazon, DeepMind and Google, Facebook, IBM, and Microsoft. Today, PAI includes for-profit technology companies,	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*Refers to Human Rights*

Organisation	Overview	RBC Issues Covered	International Instruments
	representatives of civil society, academic and research institutions, start-ups, NGOs and others in 13 countries. https://www.partnershiponai.org/		

Multi-Stakeholder social media initiatives

Organisation	Overview	RBC Issues Covered	International Instruments
VOLUNTARY INITIATIVES			
Christchurch Call	The Call outlines collective, voluntary commitments from Governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in and after the Christchurch attacks. All action on this issue must be consistent with principles of a free, open and secure internet, without compromising human rights and fundamental freedoms, including freedom of expression. It must also recognise the internet's ability to act as a force for good, including by promoting innovation and economic development and fostering inclusive societies. Founded by France and New Zealand. Supporters into states and corporate online service providers with an additional advisory group comprised of civil society. https://www.christchurchcall.com/christchurch-call.pdf	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*Refers to Human Rights*
EU Code of Practice on Disinformation	The EU Code of Practice on Disinformation (2018) involved representatives of online platforms, leading social networks, advertisers and advertising industry agreed on a self-regulatory Code of Practice to address the spread of online disinformation and fake news. The Code commitments to transparency in political advertising, the closure of fake accounts, and demonetization of purveyors of disinformation. The Code of Practice was signed by the online platforms Facebook, Google and Twitter, Mozilla, as well as by advertisers and advertising industry in October 2018 and signatories presented their roadmaps to implement the Code. In May 2019, Microsoft subscribed to the Code of Practice and also presented its roadmap.https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
Global Internet Forum to Counter Terrorism	The objective of the Global Internet Forum to Counter Terrorism (GIFCT) is to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence. The Content Incident Protocol (CIP) is a process by which GIFCT member companies become aware of, quickly assess, and act on potential content circulating online resulting from a real-world terrorism or violent extremist event. Involved parties include: DropBox, Pinterest the Hash Sharing Consortium, Microsoft, Facebook, Twitter, YouTube, Ask.fm, Cloudinary, Instagram, JustPaste.it, LinkedIn, Verizon Media, Reddit, Snap, and Yellow. https://gifct.org/press/gifct-statement-halle-shooting/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*No*
Global Network Initiative	Participants of the Global Network Initiative (GNI) commit to implement the organisation's Principles on Freedom of Expression and Privacy, which provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally. The Principles provide high-level guidance to the ICT industry on how to respect, protect, and advance user rights to freedom of expression and privacy, including when faced with government demands for censorship and disclosure of user's personal information. GNI participants include companies, academics, investors and civil society. https://globalnetworkinitiative.org/	*Disclosure, Human Rights, Labour Rights, Environment, Consumer Interests, Science and Technology, Competition*	*UNGPs, OECD*
The United Nations-	The Freedom of Expression Monitors Issued a Joint Declaration on 'Fake News', Disinformation and Propaganda that identifies the applicable human rights standards, encourages the promotion of diversity and plurality in the media, and emphasizes the particular roles played by digital	*Disclosure, Human Rights, Labour Rights, Environment,*	*UNGPs*

Organisation	Overview	RBC Issues Covered	International Instruments
OSCE, OAS, and ACHPR	intermediaries as well as journalists and media outlets. The Declaration involved the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. https://www.osce.org/fom/302796 and https://www.ohchr.org/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf	*Consumer Interests, Science and Technology, Competition*	
The Contract for the Web	This coalition of states is committed to promoting freedom of expression, association and assembly as well as the protection of privacy on the Internet - worldwide. An advisory board of civil society organizations, the private sector and academia is participating in the work of the Freedom Online Coalition (FOC) to best address issues ranging from digital inclusion, to online disinformation, the impact of cybersecurity on human rights, and the impact of Artificial Intelligence, particularly in the context of Social Media.	*Human Rights, Consumer Interests*	*UDHR, OECD*
Freedom Online Coalition (FOC)	Multi stakeholder commitment to make the Internet free, secure, accessible to all and based on human rights. It is grounded in existing human rights law and international frameworks that have been endorsed by governments around the world.	*Human Rights, Consumer Interests*	*No*
UN Secretary General's High-level Panel on Digital Cooperation	The High-level Panel on Digital Cooperation was convened by the UN Secretary-General in 2018. Its final report from June 2019 "The Age of Digital Interdependence" makes concrete recommendations on how we can work better together to realize the potential of digital technologies for advancing human well-being while mitigating the risks. The report "The Age of Digital Interdependence" refers to the 2011 Guiding Principles on Business and Human Rights and states that there is a critical need for clearer guidance about what should be expected on human rights from private companies as they develop and deploy digital technologies. According to the report, the need is especially pressing for social media companies, which is why the report's recommendation 3B calls for them to put in place procedures, staff and better ways of working with civil society and human rights defenders to prevent or quickly redress violations.https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf	*Human Rights, Consumer Interests*	*UNGPs, OECD*

Artificial intelligence guiding principles and policies by company

Company	Overview	RBC Issues Covered	International Instruments
Google (2018)	Be socially beneficial, Avoid creating or reinforcing unfair bias, Be built and tested for safety, Be accountable to people, Incorporate privacy design principles, Uphold high standards of scientific excellence; Evaluation of likely uses, including Primary purpose and use, Nature and uniqueness, Scale, and the Nature of Google's involvement	Disclosure, Human Rights, Consumer Interests	*Refers to HR*
IA Latam (2019)	AI for good; Evaluation of social impacts; Right to Privacy; Avoid bias and unfair impacts on people; Respect for Intellectual Property; Respect for the Environment; Cyber Security; Commitment to open research. Evaluation of Likely Uses based on Purpose, nature and Impact.	Disclosure, Human Rights, Consumer Interests	*No*
IBM (2019)	Accountability; Value Alignment; Explainability; Fairness; and User Data Rights	Disclosure, Human Rights, Consumer Interests	*No*
Information Technology Industry Council (ITI) (2017)	Industry's Responsibility in Promoting Responsible Development and Use; Including: Safety and Controllability, Robust and Representative Data, Interpretability and Liability of AI Systems Due to Autonomy The Opportunity for Governments to Invest in and enable the AI Ecosystem; Including: Flexible Regulatory Approach, Promoting Innovation and the Security of the Internet, Cybersecurity and Privacy, and Developing Global Standards and Best Practices The Opportunity for Public-Private Partnerships (PPPs); including: Democratizing Access and Creating Equality of Opportunity, STEM Education; and securing Future of Work	Disclosure, Human Rights, Consumer Interests	*Refers to HR*
Intel (2017)	Foster Innovation and Open Development; Create New Human Employment Opportunities and Protect People's Welfare (AI will change the way people work); Liberate Data Responsibly; Rethink Privacy; Require Accountability for Ethical Design and Implementation	Disclosure, Human Rights, Consumer Interests	*OECD*
Microsoft (2018)	Fairness, Inclusiveness, Reliability and Safety, Transparency, Privacy and Security, and Accountability	Disclosure, Human Rights, Consumer Interests	*No*
Salesforce (2019)	Responsible, Accountable, Transparent, Empowering and Inclusive	Disclosure, Human Rights, Consumer Interests	*Refers to HR*
Telefónica (2018)	Responsibility, Human Rights, Fair, Transparent and Explainable, Human Centric, Privacy and Security by Design, Policies governing work with Partners and Third-Parties	Disclosure, Human Rights, Consumer Interests	*Refers to HR*
Telia Company (2019)	Responsible and value centric, Human centric, Rights respecting, Human control, Accountable, Safe and Secure, Transparent and eEplainable, Fair and Equal, and Continuous review and Dialogue	Disclosure, Human Rights, Consumer Interests	*Refers to HR*
Workday (2019)	Respect Human rights, mitigation of bias, engagement in policy dialogue around new technologies, transparent and accountable, protection of data, privacy and ethics by design	Disclosure, Human Rights, Consumer Interests	*Refers to HR*

Social media user agreements and community standards by company

Company	Overview	RBC Issues Covered	International Instruments
Facebook	Risk Mitigation of: Violence and Criminal Behaviour; Safety; Objectionable Content; Integrity and Authenticity; Description of Data Collected and Information Shared with Third-Parties; Data Security; user Control; Accountability; Promotion of Social Good	Disclosure, Human Rights, Consumer Interests	*No*
Instagram	Risk Mitigation of: Violence and Criminal Behaviour; Safety; Objectionable Content; Integrity and Authenticity; Description of Data Collected and Information Shared with Third-Parties; Data Security; user Control; Accountability; Promotion of Social Good	Disclosure, Human Rights, Consumer Interests	*No*
LinkedIn	Fairness (mitigation of bias, ensuring non-discrimination); Accountability (Making it possible to identify and assign responsibility for a decision made by the AI system) Privacy and Confidentiality of User data, and Transparency and Explainability by Design in AI/ML Systems	Disclosure, Human Rights, Consumer Interests	*No*
Reddit	Content is prohibited if it is: illegal; pornographic; sexual or suggestive and involving minors; encouraging or inciting violence; threatening, harassing, or bullying/encouraging others to do so, personal and confidential information; impersonating someone in a misleading or deceptive manner; Using Reddit to solicit or facilitate any transaction or gift involving certain goods and services; or Is spam; in addition, prohibited behaviour includes: asking for votes or engaging in vote manipulation, Breaking Reddit or doing anything that interferes with normal use of Reddit, Creating multiple accounts to evade punishment or avoid restrictions; Reddit also enables content moderation within communities.	Disclosure, Human Rights, Consumer Interests	*No*
SnapChat	Prohibition of: content that is sexually explicit, specifically in the case of minors; Harassment and bullying including respecting people's right to privacy by not snapchatting them in private spaces and not repeatedly contacting them off of other accounts when blocked; threats, violence, and harm; Impersonation and Spam; Hate Speech and False Information including denying the existence of tragic events; illegal content; terrorist content	Disclosure, Human Rights, Consumer Interests	*No*
Twitter	Risk Mitigation of: Violence and Criminal Behavior; Safety; Objectionable Content; Integrity and Authenticity; Description of Data Collected and Information Shared with Third-Parties; Data Security; user Control; Accountability; Promotion of Social Good; Human Rights Commitments	Disclosure, Human Rights, Consumer Interests	*No*

Digitalisation and Responsible Business Conduct

Stocktaking of policies and initiatives

This paper was developed by the OECD Centre for Responsible Business Conduct as part of an ongoing consideration of the links between the digitalisation of the global economy and responsible business conduct (RBC). RBC encompasses a range of issues, including human rights abuses, consumer protection, environmental degradation, taxation, and corruption among others, as described in the OECD Guidelines for Multinational Enterprises.

http://mneguidelines.oecd.org/