OECD publishing

RIGHTS IN THE DIGITAL AGE

CHALLENGES AND WAYS FORWARD

OECD DIGITAL ECONOMY PAPERS

December 2022 **No. 347**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This paper considers the impact of digital transformation on internationally recognised human rights, legal and constitutional rights, and domestically protected interests. It considers specific case studies, and provides a brief overview of international and domestic initiatives to protect 'rights in the digital age'. Developed in the context of the 2022 Ministerial meeting of the Committee on Digital Economy Policy, this paper sets the scene for further discussion and supports policy makers in designing and achieving a rights-oriented and human-centric digital transformation.

This paper was developed by Dafna Dror-Shpoliansky (consultant to the OECD), PhD Candidate, Hebrew University of Jerusalem and a Visiting Doctoral Student at the University of Toronto, Research Fellow Federmann Cyber Security Research Center, Hebrew University, in collaboration with the OECD Secretariat (Audrey Plonk, Lisa Robinson, Gallia Daor and Nora Beauvais). It benefitted from the support of Giuseppe Bianco, Sarah Ferguson, Adam Mollerup and Alice Weber, and input from the OECD's Public Governance Directorate. Angela Gosmann, Sebastian Ordelheide and Misha Pinkhasov provided editorial support. The Ministerial meeting and related work were generously supported by the Government of Spain.

This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy on 2 December 2022 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP(2022)21/FINAL

Table of contents

Executive summary

Digital transformation affects every aspect of people's lives, individually and collectively. Technological advancement results in new business models and ways to connect, learn, create, and participate in civic spaces and the economy. It brings challenges such as breaches of privacy and the spread of illegal and harmful content online, which can diminish trust in governments and the digital environment, and undermine democratic principles. At the same time, broad and equitable access to the Internet and digital tools is essential for education, work and social engagement.

As online and offline lives intertwine, concerns and policy gaps emerge regarding individuals' needs and interests in the digital age. These can be framed from the perspective of rights, including:

- Human rights, defined by their meaning as "universal and inalienable", that all people have by virtue of existing as human beings (UN Human Rights Office, 2022[1]). Governments have obligations to protect human rights set out under international human rights law, including in the digital context (United Nations General Assembly, 2013[2]).
- Legal/constitutional rights set out in a country's domestic constitution and/or legal framework, which requires the government to recognise and protect them. These rights are not necessarily recognised as such under international human rights law.[1]
- Individual interests that are protected in a domestic context but might not be specified as a human or legal/constitutional right.

This paper considers the various types of rights and individual interests – human rights, legal and constitutional rights, and domestically protected interests – under the umbrella term "rights in the digital age". These categories can overlap, such as where an internationally recognised human right is codified in a country's constitution or legal framework (e.g. protection from discrimination).

The digital age creates novel avenues for people to exercise and enjoy their rights, but also new ways in which they can be infringed. At the same time, governments and stakeholders have raised questions regarding the protection of interests unique to the digital context (such as Internet access), including whether such interests should be protected as rights, and what such protections would entail.

In contributing to this conversation, it is helpful to ask: *Does digital transformation change traditional expectations of how governments can uphold and protect rights in the digital age? Do digital technologies compound the balancing act necessary when faced with tensions between human rights?*

This paper sheds light on how rights in the digital age relate to digital transformation and its impact on their protection. Its case studies explore how rights in the digital age are exercised and protected, including how tensions between human rights (and the necessary balancing act of protecting them) can differ between online and offline contexts. Further, it provides examples of laws and policies that encompass this concept.

Observations include:

- The digital environment poses unique risks and tensions regarding the protection of rights. Technological advances raise questions about privacy and other human rights. Similarly, the scale,

speed, and scope with which content proliferates online adds complexity to the right to freedom of expression,[2] including when it may be restricted in the interest of protecting other human rights.

- Evidence suggests increasing understanding among countries that policymaking for the digital age requires careful examination of the impact of digitalisation on the enjoyment and protection of human rights and individual interests.
- Many jurisdictions address questions of rights in the digital age through legislative and policy action. However, there are considerable variations among different approaches, with some initiatives reinforcing the principle that the same human rights that apply offline should be protected online; and others defining or elaborating specific domestic or regional guarantees, or specific frameworks, to protect individual interests and human rights in a digital context.

The OECD's whole-of-government approach, its convening power as a forum for multistakeholder engagement, and its focus on shared values positions it to advance discussion of these issues.

1. Introduction: "Rights" in online and offline contexts

Digital technologies and online environments intertwine with people's lives, aiding work, socialising, and learning (Dror-Shpoliansky and Shany, 2021[3]). Digital transformation provides many opportunities for economic growth, connecting people around the globe, elevating a sense of community, creating markets, and facilitating inclusion, such as better access to education, health, and other public services. However, it can expose people to new risks, such as security threats, privacy breaches, and restrictions on freedom of expression.

While digital technology is a recent phenomenon, rights have been part of human societies for centuries, dating back to the Cyrus Cylinder of 539 BC, the Magna Carta of 1215, and the English Bill of Rights of 1689 (Sutto, 2019[4]). In 1945, the United Nations Charter defined the purposes of the UN to include "promoting and encouraging respect for human rights and for fundamental freedoms for all" (United Nations, 1945[5]). Article 56 further stipulates all UN members' pledge of "universal respect for, and observance of, human rights and fundamental freedoms for all". Three years later, the Universal Declaration of Human Rights (UDHR) set, for the first time, a common standard of the fundamental human rights to be universally protected (United Nations, 1948[6]).

Human rights are often described as inalienable and universal (Office of the United Nations High Commissioner for Human Rights, 2022[7]), with many considered absolute. Nonetheless, the UDHR itself (along with other international human rights instruments) recognises the possibility for tension between rights in practice, which can allow for *de facto* limitations on a person's ability to exercise specific rights ("qualified rights"). In such cases, governments might be justified in restricting one right to ensure the enjoyment of another. However, such restrictions should be necessary, proportionate, and "determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society" (UDHR, Art 29). In practice, democratic countries' legal systems define how to address such situations.[3]

The speed, scale, and borderless nature of the digital environment provide a new context for understanding and exercising human rights, new ways they can be violated or abused (Dror-Shpoliansky and Shany, 2021[3]), and new ways in which their exercise may stand in tension to one another. For example, individuals can exercise the right to peaceful assembly or freedom of association online, or seek, receive and impart information and ideas through the Internet. Furthermore, digital technologies have transformed how people work, learn, access public services, and they have impacted our health and mental wellbeing (OECD, 2022[8]). At the same time, digital technologies can be used in ways that undermine the enjoyment of rights and exacerbate individual and societal harms. Arbitrary and unlawful surveillance practices, cyber and ransomware attacks, misinformation and disinformation (OECD, 2022[9]), advocacy of discriminatory hatred (constituting incitement to discrimination, violence and hostility, systemic discrimination and biases) (UN Special Rapporteur on Minority Issues, 2021[10]), and intentional disruption of Internet connectivity and government services in critical times (Access Now, 2021[11]) are examples of new threats to rights in the digital age (Citron, 2020[12]).

Instances where the protection of one human right interferes with the protection of another can manifest differently online and offline. For example, the tension between one person's right to be protected from arbitrary or unlawful interference in their private life (UDHR, Art. 12) and another's right to freedom of expression (UDHR, Art. 19) long predates the digital age. However, in the digital environment, where content can spread around the world in seconds and leave permanent digital footprints, new considerations might be warranted. Furthermore, the ubiquity of, and increasing reliance on, digital technologies can raise questions about the recognition of new human or constitutional rights (Dror-Shpoliansky and Shany, 2021[3]). For example, some jurisdictions recognise Internet access (Box 2) as a distinct right that is key to realising a spectrum of other rights.

In this regard, exercising, protecting, and promoting rights in the digital age raises unique challenges and difficult questions: *Does digital transformation change traditional expectations of how governments can uphold and protect rights in the digital age? Do digital technologies compound the balancing act necessary when faced with tension between human rights*? (OECD, 2022[13])

Due to its global and cross-cutting nature, digital transformation also raises questions regarding the roles of stakeholders. Responsibility for guaranteeing the human rights of individuals within their territory lies with the State. However, the digital environment spans multiple jurisdictions and engages the responsibility of policymakers, decisionmakers, and regulators from multiple sectors. Moreover, private actors (such as online platforms) play a central role (OECD, 2019[14]) in the practical ability of individuals to exercise certain rights in the digital age and, in accordance with the UN Guiding Principles on Business and Human Rights, have a responsibility to respect human rights in their operations (Billingham and Parr, 2020[15]) (UN Human Rights Office, 2011[16]).

The discussion of human rights, legal and constitutional rights, and individual interests in the context of digital transformation has been part of the OECD's (in particular, CDEP's) work on this topic. Notably, the 1980 Privacy Guidelines have provided guidance for over 40 years on how privacy rights should be protected in a digital context – specifically, the protection of personal data – and are the basis for privacy legislation around the world (OECD, 2013[17]). The Recommendation on Artificial Intelligence (AI) (OECD, 2019[18]) highlights the potential impact of AI development and deployment on human rights and calls on AI actors to implement mechanisms and safeguards to respect human rights. Similarly, the Recommendation on Children in the Digital Environment (OECD, 2021[19]) calls on actors to "identify how the rights of children can be protected and respected in the digital environment and take appropriate measures to do so".

This paper contributes to and facilitates dialogue between countries who share democratic values and are exploring ways to maintain and advance the enjoyment of human rights and individual interests in the digital age. It does not offer policy recommendations, but provides a launching point for dialogue and responds to the need for a further evidence-base.

Section 2 considers case studies of specific rights and how they manifest in the digital environment. It also examines the emerging trend of considering Internet access as a right, and potential implications. Section 3 considers recent domestic and international approaches to encapsulate the protection and promotion of rights in the digital age in legal and policy documents. Section 4 concludes.

In this paper, "digital age" describes developments over recent decades in which the concept of digital has gone from discrete and standalone developments to an overall transformation fully integrated in society. The paper considers the various types of rights and individual interests – human rights, legal and constitutional rights, and domestically protected interests – under the umbrella term "rights in the digital age". These categories can overlap, such as where internationally recognised human rights are codified in a country's constitution or legal framework (e.g. protection from discrimination).

2. Opportunities and challenges for rights in the digital age

The digital age provides numerous new tools, spaces, methods, and opportunities for people to enjoy rights. For example, freedom of expression cuts across society, culture and politics, and is becoming more interactive (Balkin, 2004[20]) as individuals share aspects of their lives online, from news and politics to their favourite TV shows. Individuals can respond instantly to each other, react to content posted by others, and share and comment in real time. People also have access to a variety of tools and means of expression: with a smartphone, anyone can post text or visual content on social media, start a live stream, or send voice messages (OECD, 2022[13]). Digital technologies connect people with their cultural identities, language, heritage, music, art, and family, providing expanded means to develop civic identity and engage

in political issues. Opportunities for inclusion and access to government services can be afforded to marginalised groups, such as new avenues for persons with disabilities to engage with peers and access information (OECD, 2019[21]) (OECD, 2022[22]).

These tools transform how rights such as access to education and healthcare are realised, and impact policymaking and delivery of government services (OECD, 2019[21]). In education, digital technologies provide learners with access to vast educational resources, knowledge, and information. Educational institutions use e-learning platforms to enhance educational services for students (OECD, 2019[23]) and improve understanding of their learning needs (OECD, 2019[23]). Smart technologies also contribute, such as through personalising the learning experience, supporting teachers with social robots, measuring students' engagement, or helping students with special needs participate in educational settings and practices (OECD, 2021[24]). In healthcare, digital technologies provide individuals with critical information (OECD, 2022[25]), and AI can assist in clinical decision making, public health, biomedical research, and system governance and administration (Hashiguchi, Oderkirk and Slawomirski, 2022[26]). Data increasingly drive innovation in education systems and institutions (Van der Vlies, 2020[27]), while health data can improve care quality, research, and health system management (OECD, 2016[28]).

As new technologies often outpace the policies that govern them (OECD, 2021[29]), regulatory and policy gaps create the potential for these technologies to be used in ways that harm individuals or society as a whole and undermine the enjoyment of rights in the digital age. Three examples illustrate these challenges: (1) freedom of expression, including how tensions between qualified human rights manifest; (2) privacy; and (3) the consideration of Internet access as a human or constitutional right. These examples are not exhaustive, and further work is required to comprehensively examine how digital transformation affects human rights and interests, and the potential tensions between them.

2.1. Freedom of opinion and expression, including the freedom to seek, receive and impart information in the digital age

In the digital age, individuals encounter significant threats to fully realising their "right to hold opinions without interference, and the right to freedom of expression including the right to seek, receive and impart information" (UN General Assembly, 1966[30]) ('the right to freedom of expression').

These threats include:

1. The amplification of misinformation or disinformation which can mislead the population, and interfere with the right to know and to seek and impart information, to hold opinions without interference, as well as to access reliable information (UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2021[31]) (Lesher, Pawelec and Desai, 2022[32]).
2. Dissemination of hate speech or other harmful content, and the potential tension between upholding one's right to freedom expression with ensuring that individuals can engage safely online, be protected from discrimination, and profit from equal enjoyment of the online space.
3. Unlawful restrictions on access to online content, and interference with connectivity (including Internet shutdowns), deliberately deployed to impede the right to seek, access and impart information. Some aspects of this topic are discussed also under 2.3 below.

While these concerns are not new, their scope, scale, and velocity in the digital age are unprecedented (UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2021[31]), and often result in devastating consequences for people's lives. Prominent events in recent years underscore how the widespread use of online platforms can give private companies a greater role than any government in enabling the enjoyment of the right to freedom of expression (Benesch, 2020[33]), and

how the prevalence of harmful or misleading content can pollute the information ecosystem (Shadmy, 2022[34]). Recent examples include the rapid, "infodemic" spread of disinformation and misinformation by anti-vaccine movements during COVID-19, undermining access to vital public health information (Baker, Wade and Walsh, 2020[35]), or the use of Facebook to spread a campaign of ethnic violence against the Rohingya minority in Myanmar (UN Human Rights Council, 2018[36]). These incidents raise questions about the roles of the State and private sector in respecting human rights and protecting individual and societal interests. They call on governments to consider how to address tensions between rights, such as balancing the right to freedom of expression with protection from discrimination. At the same time, they call attention to the protection of other individual interests – most prominently ensuring safety online. Such protections are essential since users are unlikely to be able to exercise their freedom of expression safely in the online environment without minimum standards in place to prevent violence and abuse.

Misinformation and disinformation

The OECD has defined 'misinformation' as false or misleading information that is shared unknowingly and is not intended to deliberately deceive, manipulate or inflict harm on a person, social group, organisation or country; and 'disinformation' as verifiably false or misleading information that is knowingly and intentionally created and shared for economic gain or to deliberately deceive, manipulate or inflict harm on a person, social group, organisation or country (Lesher, Pawelec and Desai, 2022[32]).[4] It has been observed that such content is both more likely to be spread, and more likely to be spread faster, than true content (Lesher, Pawelec and Desai, 2022[32]). A key concern for governments is tackling misinformation and disinformation and the broader, individual and societal harms it can cause, while respecting human rights.

Misinformation and disinformation can be spread by bots or trolls, including in intentional attacks (Lesher, Pawelec and Desai, 2022[32]). When combined with personalisation techniques, it can amplify disruption to public deliberation (Shadmy, 2022[34]), including by moving from online spaces (such as social media) to more traditional news sources. Such content can undermine public trust in the media, business, and government institutions (OECD, 2020[37]). It can disturb public participation in the democratic process and can intensify social polarisation, fuel fears, and lead to harmful behaviours (Lesher, Pawelec and Desai, 2022[32]) (OECD, 2020[37]). As with other digital phenomena, misinformation and disinformation are global problems that involve varied stakeholders. The OECD has noted the urgency of creating governance systems that ensure societies are resilient to misinformation and disinformation and promote information integrity more broadly (OECD, 2022[38]).

Illegal and harmful content

The faster and wider dissemination of content enabled by digital technologies has implications for people's safety and security. This includes content that is illegal in many jurisdictions, including terrorist, violent, and extremist content (TVEC), gender-based violence (GBV), and child sexual exploitation and abuse material (CSEA). At the same time, the use of digital technologies facilitates the spread of content that is not illegal, but can still cause harm (Kaye, 2019[39]) (Wong, forthcoming[40]). The latter includes cyberbullying (OECD, 2020[41]), content that promotes eating disorders and self-harm, online public shaming (Billingham and Parr, 2020[15]), harassment (Citron, 2020[12]), and trolling (Meggido, 2020[42]). Illegal and harmful content can compromise physical safety, safety online, mental health and wellbeing, and can have devastating and lifelong effects on victims and society at large. As such, the proliferation of this content impacts individuals' ability to enjoy their human rights to security of person and to non-discrimination,[5] as well as other rights and interests more broadly.

International human rights law provides a framework to address hate speech while protecting the right to freedom of expression. Responses to harmful content require carefully weighing the different rights involved. In the digital age, the decision of what is considered illegal content, and the balancing act between

harmful content and the right to freedom of speech on a day-to-day level are often left to online platforms, which operate under different content moderation mechanisms (United Nations Special Rapporteur on Freedom of Opinion and Expression, 2019[43]).

Many online platforms voluntarily implement content moderation techniques and have policies and procedures in place to address specific illegal content (for example CSEA or TVEC). The OECD took an important step in this regard, launching the Voluntary Transparency Reporting Framework, an international, standardised, transparency reporting hub that any online platform can use, regardless of its size or business model, to report on its content moderation and other techniques specific to TVEC on their platform (OECD, 2022[44]).

In parallel, some jurisdictions have sought to address concerns relating to harmful and illegal content online through laws or policies. While, in some cases, governments have legislated to address harmful or illegal content, in many jurisdictions the actions of online platforms to address such content remain voluntary (Shadmy and Shany, 2021[45]) (McCarthy, 2021[46]). Several legislative actions focus on online services having adequate systems and processes in place to prevent harm, rather than on reactive procedures to remove harmful or illegal content after the fact. As legislation develops and tools to combat harmful and illegal content evolve, it will be important for governments to consider the impact of tools that could result in limitations on human rights, including the right to freedom of expression for the purpose of protecting the safety of others. Or indeed, how to balance the right to freedom of expression when that speech is harmful and could limit others' ability to speak and participate online.

Approaches to regulating harmful content can vary significantly, as in the case of image-based abuse[6] – the distribution of sexually graphic images of individuals without their consent (Citron, 2020[12]). While image-based abuse is criminalised in some jurisdictions (for example, Australia, Canada, Israel) (Government of Israel, 2014[47]) (Government of Canada, 2015[48]) (Government of Australia, 2021[49]) (CEDAW, 2016[50]), it remains in the hands of online platforms in other countries, which has led to harmful consequences for the persons involved in some instances. While many platforms have rules to remove this type of content, this does not always provide appropriate safeguards and is not always expedient. For example, the "Facebook Papers" revelations reported that a nude photo of a woman was reposted 50 million times before it was removed (Horowitz, 2021[51]). Box 1 discusses emerging laws and policies to address online safety.

Box 1. Measures to advance safety online

Ever more jurisdictions are implementing laws and policies to advance safety online. These often centre on the activities of online platforms and propose that they have systems and processes to keep users safe; have transparency requirements; make it easier to report illegal content and have it removed; and impose sanctions should requirements not be respected.

Many proposals include measures to address specific harms, such as gender-based or intimate partner violence, or threats to child safety. The recent EU proposal for a directive on combatting violence against women and domestic violence specifically addresses online violence. Australia's Online Safety Act (Government of Australia, 2021[49]) has provisions related to image-based abuse, cyberbullying, TVEC and CSEA. The Act sets out Basic Online Safety Expectations, and requires online platforms to address harms that can violate human rights. Australia's eSafety Commissioner can require platforms to report on the steps they take to comply with the Basic Online Safety Expectations and proactively minimise material or activity that is unlawful or harmful. The proposed EU Regulation laying down rules to prevent and combat child sexual abuse specifically targets the protection of children (European Commission, 2022[52]). Similarly, the United Kingdom's Online Safety Bill contains measures to tackle content that is illegal and harmful to children. In Colombia, laws require blocking illegal content such as

CSEA, or illegal gambling (Government of Colombia, 2001[53]). Canadian online service providers must report CSEA detected on their system (Government of Canada, 2011[54]).

Promoting a safe and trustworthy digital environment is the subject of several high-level statements. In April 2021, G7 Digital Technology Ministers adopted Internet Safety Principles (G7, 2021[55]) which recognised that "online content that is illegal, and content that is harmful, can have a major impact on people, especially women and children, and on our societies". These principles emphasise the importance of transparency and accountability and urge companies to put systems and processes in place to improve Internet safety and reduce illegal and harmful content and activity on their platforms. Most recently, the 2022 G20 Leaders' Declaration affirmed that "a resilient, safe and secure online environment is necessary to enhance confidence and trust in the digital economy" (G20, 2022[56]).

These actions follow the 2019 G7 Digital Ministers Meeting (G7, 2019[57]), which noted the growing prevalence of online harms and called for more to be done to enhance accountability and transparency while protecting and promoting human rights. The G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism, and the 2021 G7 Statement on Preventing and Countering Violent Extremism and Terrorism Online urged platforms to be more ambitious in playing their part and underscored the importance of a multistakeholder approach, inclusive of governments, academia, civil society, and industry (G7, 2021[58]) (G20, 2019[59]). The Christchurch Call (Christchurch Call, 2019[60]), which takes a multistakeholder approach, sets out commitments for companies and governments to make in this area.

Given the scope, breadth, and velocity with which content can spread online, effective content moderation remains a significant challenge. Efforts by some online platforms to use automated systems that detect and remove illegal content (Benesch, 2020[33]) have been criticised for errors, bias and over-filtering (Gillespie, 2020[61]), and can have limited capacity to understand the context in which content is shared. Meanwhile, despite more online platforms issuing transparency reports, these remain limited and companies use different definitions, metrics and reporting frequencies, and it can be difficult to verify compliance with self- or co-regulatory requirements. As a result, it is difficult to gain an industry-wide perspective on the efficacy of such measures, and to assess their impact on human rights (OECD, 2022[62]). Another concern regarding self-regulation practices (Medzini, 2022[63]) is that businesses may be motivated by financial interests rather than accountability (Suzor and Gillett, 2022[64]), although it is worth recognising the business interest in ensuring that services are safe and welcoming to users (OECD, 2021[65]). The OECD contributes to the evidence base of approaches of online content services to combat illegal content, focusing on TVEC (OECD, 2021[66]) and CSEA.

Content moderation by online platforms provides an illustrative case study of the challenges around the enjoyment and protection of rights in the digital age, notably considering its cross-border nature. While countries enforce their national laws in their jurisdictions, online platforms tend to operate globally. As rules pertaining to activities in the digital environment vary between jurisdictions, this can lead to conflicting regulatory requirements for online platforms and to enforcement gaps (OECD, 2021[29]) (OECD, 2022[67]). A user might post content that is illegal in one jurisdiction, but if the website is hosted in another, that puts it out of reach for the government to enforce its laws (Kohl, 2021[68]). At the same time, legal requirements in one country could unduly curtail freedom of expression, and not be accepted in another. Liability rules can also differ between countries. Section 230 of the US Communications Decency Act (Government of the United States, 1996[69]) limits the liability of platforms for content published by their users (Bedell and Major, 2020[70]) and enables them to moderate content. In Germany, the Network Enforcement Law (NetzDG) requires certain social media platforms to remove illegal and other specified harmful content within a limited time and can impose fines for noncompliance (Kohl, 2021[68]).[7]

Internet shutdowns and restrictions

Internet shutdowns and restrictions are intentional measures to "prevent or disrupt accesses to or dissemination of information online." Their active, deliberate nature distinguishes them from divides in digital access that arise from a lack of infrastructure or capacity. Intentional Internet disruptions can involve mass blocking of platforms and messaging services, the closure of a network or specific websites, and the imposition of differentiated restrictions on online access (UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2021[31]). These actions likely impinge on individuals' right to freedom of expression by limiting or entirely cutting off their capacity to seek, receive, and impart information. Along with the impact on the enjoyment of human rights, Internet shutdowns and restrictions have significant economic implications. For example, Internet shutdowns are estimated to have cost the Indian economy over $960 million in 2016 (West, 2016[71]).

Restrictions on Internet access are often introduced in politically sensitive times. For example, according to the UN Rapporteur for the Right to Free Expression, Tajikistan blocked access to messaging services and social media operating outside its territory during public protests (UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2016[72]). Intentional network disruptions were reported in Gabon during the election period (UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2017[73]), and the Russian government recently blocked access to prominent online platforms, reportedly in an effort to promote national propaganda and block other channels of information (Budnitsky, 2022[74]).

2.2. Privacy and protection of personal data

The implications of the digital age for privacy rights have been widely discussed. The right to privacy is protected by Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which protects people from "arbitrary or unlawful interference with" one's "privacy, family, home or correspondence" and from "unlawful attacks" on one's "honour and reputation" (UN General Assembly, 1966[30]).

The UN Human Right Committee's 1988 General Comment No. 16 elaborates on Article 17 by explaining terms such as "unlawful", "arbitrary interference", and "family". It also recognises the "gathering and holding of personal information on computers, data banks and other devices" (United Nations, Human Rights Committee, 1988[75]).

The OECD has promoted respect for privacy and protection of personal data for over four decades, spurring development of policy frameworks to address challenges that stem from digital transformation. The OECD's Privacy Guidelines establish the basic principles for privacy protection, with a view to promoting trust and facilitating cross-border flows of personal data (OECD, 2013[17]).

Digital technology alters the way personal data are used and calls into question foundational aspects of protecting privacy and personal data online, including consent, purpose limitation, and even the very definition of personal data (OECD, 2021[76]). For example, the ability to customise the content and experience of users online can make interactions in the digital environment more efficient and enjoyable. However, this raises questions about the intrusiveness of those technologies (Zuboff, 2019[77]) and about transparency regarding third-party access to and use of data.

Much of the recent debate on privacy focuses on whether current policies sufficiently address contemporary threats to individual privacy (Clifford, Richardson and Witzleb, 2021[78]). Among other considerations, this refers to: online content-sharing services' ability to personalise content for each user (known as microtargeting) (Gordon-Tapiero, Wood and Ligett, 2022[79]); the advent of inferential analytics such as AI technology that generates sensitive information via inferences; facial recognition technology in public spaces; and technologies that can purportedly deduce information such as sexual orientation,

political affiliation, and so on without users willingly providing this information or even being aware it can be gathered (UN Special Rapporteur on the right to privacy, 2018[80]).

2.3. Connectivity and digital divides: an emerging right to access?

In addition to promoting the opportunities that digital transformation brings and safeguarding individuals from potential harms, the digital age poses questions about emerging issues and concepts related to rights. One example is equitable access to communications infrastructures, services and data – delivered by both private and public actors – that underpin digital transformation and increasingly become a gateway for people to exercise their rights.

Indeed, access to Internet has become essential for education, work, public services, and social interactions. The COVID-19 pandemic put this into focus when access to high-quality broadband (OECD, 2021[81]) was of crucial importance, constituting the only channel to realise other rights. During the pandemic, not all populations had the opportunity to continue exercising and enjoying their human rights due to a lack of connectivity, mostly in developing and least-developed countries – although gaps also remain in OECD countries (OECD, 2021[82]) (OECD, 2022[83]). According to 2021 figures, 2.9 billion people – 37 percent of the world's population – have never used the Internet, a phenomenon known as the "digital divide" (ITU, 2021[84]).

While there is no recognised human right to access the Internet, a number of countries and international organisations (OSCE, 2019[85]) have recently acknowledged the importance of Internet access and explained some particular interests and features that should be protected (Dror-Shpoliansky and Shany, 2021[3]) (Box 2).

Beyond ensuring widespread connectivity and access to the digital environment, meaningful access requires that people have adequate digital literacy and skills to use digital technologies, and that they are empowered to realise its benefits and understand its risks (Çalı, 2020[86]). Addressing digital divides therefore goes beyond Internet connectivity, and improving indicators such as income, employment and education can have a direct impact on gaps in digital access (OECD, 2022[83]).

Box 2. A right to Internet access?

In 2011, the UN Rapporteur on the right to freedom of expression emphasised that Internet access has two dimensions (UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2011[87]): (1) access to an Internet connection, which generally refers to technical infrastructure and equal access to connectivity (UNDP, 2021[88]) (OECD, 2021[81]); and (2) access to online content, which refers to protection from disruption to online content, for example due to intentional shutdowns or restrictions.

In 2020, UNESCO reaffirmed the need for Internet universality (UNESCO, 2022[89]). The EU incorporated Internet access into its proposed Declaration on Digital Rights and Principles for the Digital Decade (European Commission, 2022[90]). In addition, the Organization of American States (OAS), the Council of Europe, and the African Commission on Human and Peoples' Rights all repeatedly emphasised the importance of access as indispensable to realising other human rights. Colombia, Estonia, Finland, Greece, Mexico, and Spain all incorporated the right to access in their legislation (Psaila, 2011[91]) (Government of Mexico, 2021[92]) (Government of Colombia, 2021[93]).

The OECD Recommendation on Broadband Connectivity sets out measures to eliminate digital divides, such as fostering the use of broadband at affordable prices and strengthening consumer rights via competition in the communication services market (OECD, 2021[81]). The OECD Recommendation on

Digital Government Strategies recommends that governments take steps that address digital divides in the provision of government services and avoid new forms of digital exclusion (OECD, 2014[94]).

3. Protections for rights in the digital age

Recent years have seen growing domestic and international policy focus on promoting and protecting human rights in digital transformation. The 2021 Statement of the OECD Meeting of the Council at Ministerial level called "upon the OECD to promote the use of technology that respects data privacy and intellectual property rights, ensures the safety and security of users, especially youth, counters disinformation, and protects democratic principles and human rights" (OECD, 2021[95]). This section examines domestic, regional, and international initiatives and briefly sets out the current state of play regarding legal and policy measures to safeguard rights and address related challenges in the digital age.[8] It also considers the role of business.[9]

3.1. Domestic initiatives

Several countries have developed laws or policies that seek to address the protection of human rights and individual interests in the digital age. Some seek to address new challenges through legal guarantees such as new or amended laws to protect personal data (Conseil d'État, 2016[96]). Others consider the question holistically, launching broad initiatives to protect rights in the digital age and promote a human-centric digital transformation. Some jurisdictions are exploring new rights in specific domains, such as algorithmic transparency and accountability in AI decision making. At the same time, many countries approach digital transformation with a focus on existing normative sources and human rights frameworks, emphasising that human rights are protected offline and must be protected online (OECD, 2022[97]).

Examples of a dedicated domestic policy approach to 'digital rights' include Spain, Portugal, Brazil, and Italy. Spain applies an overarching policy umbrella, encompassing laws, regulations, public policies, principles, and commitments to uphold human-centric digital transformation and rights in the digital age. The 2021 Charter for Digital Rights protects and adapts existing human rights and individual interests in the digital environment across jurisdictions, ensures cross-government alignment, and advances new rights emerging in the digital context. For example, it sets out the right not to be traced and profiled, the right to cybersecurity, the right to disconnect, and the right to digital inheritance (Government of Spain, 2021[98]).

Similarly, the Portuguese Charter of Human Rights in the Digital Age (Government of Portugal, 2021[99]) sets out rights and duties between the State and citizens, and between private individuals, specific to the digital environment. The Portuguese Charter includes human rights (e.g. freedom of expression, privacy) and directs how to apply them in a digital setting. Like the Spanish Charter, it sets out new rights such as a users' right to net neutrality, the right to a digital will, and the right to be forgotten.

Brazil's Internet Bill of Rights likewise protects internet privacy and free expression, and new rights, like net neutrality (Government of Brazil, 2014[100]). Italy's Declaration of Internet Rights (Government of Italy, 2015[101]) considers existing rights such as privacy, identity, or self-determination within a digital context and elaborates new ones, like the rights of people on platforms, and Internet governance. Colombia declared Internet access an essential public service (Government of Colombia, 2021[93]), and Mexico included it as a constitutional right (Government of Mexico, 2021[92]).[10]

New rights for a digital context

Some countries have sought to elaborate new rights specific to the digital world, in relation to "rights that protect online needs and interests that do not have close parallels in the offline world". According to Dror-Shpoliansky and Shany's proposed typology, the rationale of these categories of rights is to protect unique needs and interests that may not be fully or adequately covered by existing rights frameworks (Dror-Shpoliansky and Shany, 2021[3]). Some do this by articulating new rights in overarching bills or charters (e.g. the cases of Italy, Portugal, Spain, and Brazil mentioned above). Others do so as a standalone effort or by incorporation into other laws (e.g. within the constitution). Chile is the first country to include "brain rights" in its constitution, with the aim of protecting mental privacy, free will, and non-discrimination in access to neurotechnology (Government of Chile, 2021[102]) (OECD, 2022[103]).

Technology-related rights

Laws or policy proposals have been introduced regarding specific technologies, such as pertaining to AI or automated decision-making. Japan focuses on specific recommendations in this regard (Government of Japan, 2022[104]). The United States developed a Blueprint for an AI Bill of Rights (The White House, 2022[105]). Colombia has an Ethical Framework for Artificial Intelligence (Government of Colombia, 2021[106]).

3.2. Regional and international initiatives

Recent initiatives at regional and international levels affirm States' obligation to protect human rights online and offline. In 2012, the UN Human Rights Council (HRC) recognised that "the same rights people have offline must also be protected online" (United Nations Human Rights Council, 2012[107]). This position was subsequently reaffirmed by the HRC and the UN General Assembly (UNGA).[11] These resolutions express a "normative equivalency" approach, as termed by Dror-Shpoliansky and Shany, and centre the issue around finding ways to extend, adopt and apply existing, traditional, international human rights from the analogue to the digital world, by means of interpretation (Dror-Shpoliansky and Shany, 2021[3]).

International human rights law provides a framework for protecting individual rights and interests in the digital environment. This framework is found in the instruments themselves (e.g. UDHR and ICCPR) and the jurisprudence of human rights committees and bodies that provide recommendations, opinions, and other interpretive texts about the application of international human rights law to the digital context (Seibert-Fohr, 2018[108]). For example, the UN High Commissioner for Human Rights and the UN Human Rights Committee have issued reports on privacy rights in the digital environment, such as on the public-space nature of the Internet, privacy protections relevant to metadata, and surveillance powers of States (Office of the United Nations High Commissioner for Human Rights, 2018[109]) (United Nations Human Rights Committee, 2019[110]).

In 2021, the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE), reaffirmed that countries need to respect and protect human rights and fundamental freedoms offline and online with regard to the use of information and communications technologies (ICTs), in accordance with the HRC and UNGA resolutions (UN Group of Governmental Experts (GGE), 2021[111]). Likewise, the Freedom Online Coalition – a group of governments that support Internet freedom, and protect freedom of expression, association, assembly and privacy online – is committed to the principle that the human rights people have offline are the same online (Freedom Online Coalition, 2021[112]).

Other international efforts set out a framework for applying existing rights standards to a digital context, and some incorporate new digital rights (such as to access). These include the UN High-Level Panel for Digital Co-Operation (United Nations, n.d.[113]), the declaration of the World Summit on the Information

Society (WSIS) (World Summit on the Information Society Forum, 2003[114]), and the Charter of Human Rights and Principles for the Internet (a collaborative initiative by the UN Internet Governance Forum and Internet Rights and Principles Coalition from 2014) (Internet Rights and Principles Dynamic Coalition, 2014[115]). The Council of Europe's Guidelines to respect, protect and fulfil the rights of the child in the digital environment (CoE, 2018[116]), and the Committee on the Rights of the Child General Comment on children's rights in the digital environment (Committee on the Rights of the Child, 2021[117]) provides interpretive guidance on how to protect children's rights in the digital environment.

The European Commission's proposal for a European Declaration on Digital Rights and Principles for the Digital Decade spells out shared political intentions and commitments as well as recalls and gives guidance on applying existing rights in the digital environment. It provides guidance on the promotion and protection of human rights (such as the right to freedom of expression) in a digital context, and outlines commitments, such as regarding digital connectivity, and interactions with algorithms and AI systems (European Commission, 2022[90]). At the EU level, the General Data Protection Regulation (GDPR) (European Commission, 2018[118]) sets out further (or 'new') rights within the frame of the right to privacy, including the right not to be subject to a decision based solely on automated processing, the right to data portability, and the right to erasure.[12]

The proliferation of initiatives concerning rights, values and interests in the digital age underscores the shared and global nature of the policy and enforcement challenges that it poses. While multiple governments, organisations, and rights bodies seek to address these challenges within a rights framework, variations exist among their approaches. While some initiatives reinforce the idea that existing human rights law provides the framework to protect rights, others define or elaborate specific new rights in policy or domestic law, and others set out specific frameworks for rights in the digital age. Many initiatives use the same document to set out how to apply existing human rights in the digital age and to elaborate new ones.

There is an increasing understanding among governments and international human rights bodies that protecting human rights and individual interests in the digital age might require new laws, policies, and strategies. However, there is not yet a coherent position as to how this can be achieved, and the evidence-base setting out gaps and challenges is still evolving.

3.3. Responsibility of business

Several initiatives set out the role of business in respecting and promoting human rights. Most prominently, the UN Guiding Principles on Business and Human Rights (the Guiding Principles) is a non-binding, international instrument that sets out the responsibility of transnational corporations and other businesses to respect internationally recognised human rights. This includes making policy commitments, engaging in prevention, and conducting due diligence to identify human rights impacts. In parallel, the Guiding Principles say that States have a duty to ensure that businesses domiciled in their territory and/or jurisdiction respect human rights (UN Human Rights Office, 2011[16]).The UN Office of the High Commissioner for Human Rights' B-Tech Project provides guidance and resources for implementing the Guiding Principles in the technology space (Office of the United Nations High Commissioner for Human Rights, 2021[119]).

Consistent with the Guiding Principles, the OECD Guidelines for Multinational Enterprises (MNE Guidelines) state that enterprises should respect human rights, and offer specific recommendations. For example, enterprises should avoid infringing on the human rights of others; address potential or actual adverse human rights impacts linked to their operations, products, or services; mitigate risks in this regard; make policy commitments to respect human rights, carry out human rights due diligence, and co-operate with legitimate processes in the remediation of adverse human rights impacts should they have caused or

contributed to them (OECD, 2011[120]). A targeted update of the OECD MNE Guidelines is ongoing, including the chapter on science and technology.

Finally, the OECD Recommendation on Children in the Digital Environment addresses the essential role of digital service providers (OECD, 2021[121]) in providing a safe and beneficial digital environment for children. Accompanying the Recommendation, the Guidelines for Digital Service Providers support digital service providers when they take actions that may directly or indirectly affect children in the digital environment, particularly in determining how best to respect their human rights, safety, and interests.

4. Conclusions

Rapid technological developments have progressed much faster in recent decades than the policies that govern them. This accelerating transformation provides opportunities and risks for the enjoyment of rights in the digital age. It also presents challenges to the fulfilment of governments' obligations under binding international human rights frameworks, and in their domestic legal frameworks.

Examining the rights to freedom of expression and to privacy unearths several risks and tensions in a digital context. These include the negative impact of misinformation and disinformation and harmful content on the freedom of expression, and the complexity that new technologies raise around privacy and protection. Examining the emerging discussion around a "right to access" considers Internet access itself as a gateway to the fulfilment of other rights, and as a possible bellwether for the discussion of digital-specific rights.

There is growing interest in rights as a lens for considering policies for digital transformation. Emerging approaches indicate that the conceptualisation of rights in the digital age is fragmented, which can have implications on the coherence of efforts to promote them. At the same time, guidance from international human rights bodies is clear that human rights must be protected off- and online. However, the question remains as to how governments can navigate the digital sphere and adapt their actions to ensure the continued protection of human rights, legal and/or constitutional rights, and individual interests.

In this regard, understanding is increasing among countries that upholding and protecting rights in the digital age requires close examination of the impact of digitalisation on the enjoyment and protection of rights, and on the interplay between them. While some jurisdictions seek to address rights questions within existing normative frameworks, others consider that this calls for specific laws, policies, strategies, and even new rights designed for individuals' activities in the digital environment.

This paper provides a point of departure for considering rights in the digital age. Looking forward, our challenge as a society is to find an adequate approach that enables innovation and can ensure it is safe, accountable, human-centred, and rights-oriented. The OECD's whole-of-government approach, convening power as a forum for multi-stakeholder engagement, and focus on like-mindedness and shared values make it well-suited for advancing discussion on these issues.

References

Access Now (2021), *#KeepItOn: Fighting internet shutdowns around the world*, https://www.accessnow.org/keepiton/. [11]

Australian eSafety Commissioner (n.d.), *Image Based Abuse*, https://www.esafety.gov.au/research/image-based-abuse. [124]

Baker, S., M. Wade and M. Walsh (2020), "The challenges of responding to misinformation during a pandemic: Content moderation and the limitations of the concept of harm", *Media International Australia*, Vol. 177/1, pp. 103-107, https://doi.org/10.1177/1329878X20951301. [35]

Balkin, J. (2004), *How Rights Change: Freedom of Speech in the Digital Era*, https://openyls.law.yale.edu/bitstream/handle/20.500.13051/1734/How_Rights_Change_Freedom_of_Speech_in_the_Digital_Era.pdf?sequence=2. [20]

Bedell, Z. and J. Major (2020), *What's Next for Section 230? A Roundup of Proposals*, https://www.lawfareblog.com/whats-next-section-230-roundup-proposals. [70]

Benesch, S. (2020), "But Facebook's not a country: How to interpret human rights law for social media companies", *Yale Journal on Regulation Bulletin*, Vol. 38, pp. 86-111, https://ssrn.com/abstract=3692701. [33]

Billingham and Parr (2020), *Enforcing social norms: The morality of public shaming*, https://onlinelibrary.wiley.com/doi/full/10.1111/ejop.12543. [15]

Budnitsky, S. (2022), *Kremlin tightens control over Russians' online lives – threatening domestic freedoms and the global internet*, https://theconversation.com/kremlin-tightens-control-over-russians-online-lives-threatening-domestic-freedoms-and-the-global-internet-182020. [74]

Çalı, B. (2020), *The case for the right to meaningful access to Internet as a Human Right in International Law*, Cambridge University Press, https://doi.org/10.1017/9781108676106.022. [86]

CEDAW (2016), *Most Victims of 'Revenge Porn' Targeted by Partners*, http://www.cedaw.org.tw/en/en-global/news/detail/104. [50]

Christchurch Call (2019), , https://www.christchurchcall.com/. [60]

Citron, D. (2020), "Cyber Mobs, Disinformation, and Death Videos: The Digital environment as It Is (and as It Should Be)", *Michigan Law Review*, Vol. 118/6, pp. 1073-1094, https://doi.org/10.36644/mlr.118.6.cyber. [12]

Clifford, D., M. Richardson and N. Witzleb (2021), *Artificial Intelligence and Sensitive Inferences: New Challenges for Data Protection Laws*, Edward Elgar Publishing Limited, https://doi.org/10.4337/9781800880788. [78]

CoE (2018), "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a. [116]

Committee on the Rights of the Child (2021), *General Comment no. 25 on Children's Rights in Relation to the Digital Environment*, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. [117]

Conseil d'État (2016), "Fundamental rights in the Digital Age", https://www.conseil-etat.fr/en/Media/actualites/documents/reprise-_contenus/rapports-et-etudes/fundamental-rights-in-the-digital-age.pdf. [96]

Dror-Shpoliansky, D. and Y. Shany (2021), "It's the end of the (offline) world as we know it: from human rights to digital human rights - a proposed typology", *European Journal of International Law*, Vol. 32/4, pp. 1249-1282, https://doi.org/10.1093/ejil/chab087. [3]

European Commission (2022), *European Digital Rights and Principles*, https://digital-strategy.ec.europa.eu/en/policies/digital-principles#tab_2. [90]

European Commission (2022), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472. [52]

European Commission (2018), *General Data Protection Regulation*, https://eur-lex.europa.eu/eli/reg/2016/679/oj. [118]

Freedom Online Coalition (2021), *Aims & Priorities*, https://freedomonlinecoalition.com/aims-and-priorities/. [112]

G20 (2022), *Bali Leader's Declaration*, https://reliefweb.int/report/world/g20-bali-leaders-declaration-bali-indonesia-15-16-november-2022. [56]

G20 (2019), *G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism*, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_statement_on_preventing_terrorist_and_vect.html. [59]

G7 (2021), *Internet Safety Principles*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986161/Annex_3__Internet_Safety_Principles.pdf. [55]

G7 (2021), *Statement on Preventing and Countering Violent Extremism and Terrorism Online*, https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/annex-1-statement-on-preventing-and-countering-violent-extremism-and-terrorism-online-accessible-version. [58]

G7 (2019), *Digital Ministers Meeting*, https://www.economie.gouv.fr/files/files/2019/G7/G7Num/Chairs_summary_version_finale_ENG.pdf. [57]

Gillespie, T. (2020), "Content moderation, AI, and the question of scale", *Big Data & Society*, Vol. 7/2, https://doi.org/10.1177/2053951720943234. [61]

Gordon-Tapiero, A., A. Wood and K. Ligett (2022), "The Case for Establishing a Collective Perspective to Address the Harms of Platform Personalization", *Vanderbilt Journal of Entertainment & Technology Law*, https://ssrn.com/abstract=4105443. [79]

Government of Australia (2021), *Online Safety Act*, https://www.legislation.gov.au/Details/C2021A00076. [49]

Government of Brazil (2014), *Marco Civil Law of the Internet in Brazil*, https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180. [100]

Government of Canada (2015), *Non-Consensual Distribution of Intimate Images Section 162.1*, https://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-46/latest/rsc-1985-c-c-46.html#sec162.1. [48]

Government of Canada (2011), *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*, https://laws-lois.justice.gc.ca/eng/acts/I-20.7/FullText.html. [54]

Government of Chile (2021), *Constitutional Amendment on Neuro-Rights*, https://static1.squarespace.com/static/60e5c0c4c4f37276f4d458cf/t/6182c0a561dfa17d0ca34888/1635958949324/English+translation.pdf. [102]

Government of Colombia (2021), *Ethical Framework for Artificial Intelligence in Colombia*, https://inteligenciaartificial.gov.co/en/ethical-framework/. [106]

Government of Colombia (2021), *Ley 2108 de 2021, Ley de Internet como servicio público esencial y universal' o por medio de la cual se modifica la Ley 1341 de 2009 y se dictan otras disposiciones*, https://vlex.com.co/vid/ley-2108-2021-ley-873893433. [93]

Government of Colombia (2001), *Ley 679 de 2001 por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.*, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=18309. [53]

Government of Israel (2014), *Prohibition of Online Distribution of Sexual Images Without Consent*, https://www.loc.gov/item/global-legal-monitor/2014-01-10/israel-prohibition-of-online-distribution-of-sexual-images-without-consent/. [47]

Government of Italy (2015), *Declaration of Internet Rights*, https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf. [101]

Government of Japan (2022), *Governance Guidelines for Implementation of AI Principles*, https://www.meti.go.jp/english/press/2022/0128_003.html. [104]

Government of Mexico (2021), *Constitucion Politica de los Estados Unidos Mexicanos*, http://www.ordenjuridico.gob.mx/constitucion.php#gsc.tab=0. [92]

Government of Portugal (2021), *Carta Portuguesa de Direitos Humanos na Era Digital (Lei n.º 27/2021, de 17 de maio)*, https://dre.pt/dre/detalhe/lei/27-2021-163442504. [99]

Government of Spain (2021), *Charter of Digital Rights*, https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf. [98]

Government of the United States (1996), *US Communications Decency Act (47 US Code Section 230)*, https://www.govinfo.gov/content/pkg/USCODE-2020-title47/pdf/USCODE-2020-title47-chap5-subchapII-partI-sec230.pdf. [69]

Hashiguchi, T., J. Oderkirk and L. Slawomirski (2022), "Fulfilling the Promise of Artificial Intelligence in the Health Sector: Let's Get Real", https://doi.org/10.1016/j.jval.2021.11.1369. [26]

Horowitz, J. (2021), *The Facebook Files, Part 1: The Whitelist*, https://www.wsj.com/podcasts/the-journal/the-facebook-files-part-1-the-whitelist/aa216713-15af-474e-9fd4-5070ccaa774c?mod=article_inlin. [51]

Internet Rights and Principles Dynamic Coalition (2014), *The Charter of Human Rights and Principles for the Internet*, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf. [115]

ITU (2021), *Facts and Figures 2021: 2.9 billion people still offline*, https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline/. [84]

Kaye, D. (2019), *Speech Police: The Global Struggle to Govern the Internet*, Columbia Global Reports, https://doi.org/10.2307/j.ctv1fx4h8v. [39]

Kohl, U. (2021), *Jurisdiction in Network Society*, Edward Elgar Publishing, https://doi.org/10.4337/9781789904253. [68]

Lesher, M., H. Pawelec and A. Desai (2022), *Disentangling untruths online: Creators, spreaders and how to stop them*, https://doi.org/10.1787/84b62df1-en. [32]

McCarthy, N. (2021), *The Governments Trying To Remove Reddit Content*, https://www.forbes.com/sites/niallmccarthy/2021/02/18/the-governments-trying-to-remove-reddit-content-infographic/?sh=636fe240e714. [46]

Medzini, R. (2022), "Enhanced self-regulation: The case of Facebook's content governance", *New Media & Society*, Vol. 24/10, pp. 2227-2251, https://doi.org/10.1177/1461444821989352. [63]

Meggido, T. (2020), *Online Activism, Digital Domination and the Rule of Trolls*, https://www.academia.edu/40450929/Online_Activism_Digital_Domination_and_the_Rule_of_Trolls. [42]

Ministry of Science and ICT, Republic of Korea (2022), *대한민국 디지털 전략 발표, [Korea Digital Strategy Announcement]*, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=3&bbsSeqNo=94&nttSeqNo=3182193&searchOpt=ALL&searchTxt= (accessed on 24 October 2022). [122]

OECD (2022), *Building better societies through digital policy: Background paper for the CDEP Ministerial meeting", OECD Digital Economy Papers*, OECD Publishing, https://doi.org/10.1787/07c3eb90-en. [83]

OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, https://doi.org/10.1787/76972a4a-en. [38]

OECD (2022), *Companion Document to the OECD Recommendation on Children in the Digital Environment*, OECD Publishing, Paris, https://doi.org/10.1787/a2ebec7c-en. [22]

OECD (2022), "Focus on rights in the digital age", https://www.oecd.org/digital/rights/. [97]

OECD (2022), "ICT Access and Usage by Households and Individuals", *OECD Telecommunications and Internet Statistics* (database), https://doi.org/10.1787/b9823565-en (accessed on 18 October 2022). [25]

OECD (2022), *OECD Global Forum & Public Governance Ministerial Meeting. Reinforcing Democracy and Building Trust*, https://www.oecd.org/governance/reinforcing-democracy/. [9]

OECD (2022), *OECD Workshop on Rights in the digital age "Standing our Ground: a common dialogue on digital rights"*, https://www.oecd.org/digital/rights/rights-in-the-digital-age-workshop-1-agenda.pdf. [103]

OECD (2022), *Putting People First: a background paper for the CDEP Ministerial Meeting*, https://doi.org/10.1787/865f8426-en. [13]

OECD (2022), *Recommendation on International Regulatory Co-operation to Tackle Global Co-operation*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0475. [67]

OECD (2022), *Rights in the Digital Age*, https://www.oecd.org/digital/rights/. [8]

OECD (2022), *Transparency Reporting on Terrorist and Violent Extremist Content Online, 3rd edition*, https://doi.org/10.1787/a1621fc3-en. [62]

OECD (2022), *Voluntary Transparency Reporting Framework (VTRF) Glossary*, https://www.oecd-vtrf-pilot.org/glossary#glossary-content-sharing-services. [44]

OECD (2021), *Bridging connectivity divides*, https://www.oecd.org/fr/concurrence/bridging-connectivity-divides-e38f5db7-en.htm. [82]

OECD (2021), *Guidelines for Digital Service Providers*, https://legalinstruments.oecd.org/public/doc/272/5803627d-b49b-4894-8dbe-35f67fd10007.pdf. [121]

OECD (2021), *Meeting of the OECD Council at Minsiterial Level (Statement)*, https://www.oecd.org/mcm/2021/MCM-2021-Part-2-Final-Statement.EN.pdf. [95]

OECD (2021), *OECD Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots*, OECD Publishing, Paris, https://doi.org/10.1787/589b283f-en. [24]

OECD (2021), *Practical Guidance on Agile Regulatory Governance to Harness Innovation*, https://legalinstruments.oecd.org/public/doc/669/9110a3d9-3bab-48ca-9f1f-4ab6f2201ad9.pdf. [65]

OECD (2021), *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [29]

OECD (2021), *Recommendation of the Council on Broadband Connectivity*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0322. [81]

OECD (2021), *Recommendation of the Council on Children in the Digital Environment*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [19]

OECD (2021), *Report on the implementation of the Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, https://one.oecd.org/document/C(2021)42/en/pdf. [76]

OECD (2021), *Transparency reporting on terrorist and violent extremist content online*, https://www.oecd.org/digital/transparency-reporting-on-terrorist-and-violent-extremist-content-online-8af4ab29-en.htm. [66]

OECD (2020), "Protecting children online: An overview of recent developments in legal frameworks and policies", *OECD Digital Economy Papers*, No. 295, OECD Publishing, Paris, https://doi.org/10.1787/9e0e49a9-en. [41]

OECD (2020), *Transparency, communication and trust: The role of public communication in responding to the wave of disinformation about the new coronavirus*, https://www.oecd.org/coronavirus/policy-responses/transparency-communication-and-trust-the-role-of-public-communication-in-responding-to-the-wave-of-disinformation-about-the-new-coronavirus-bef7ad6e/. [37]

OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, https://www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.htm. [14]

OECD (2019), *OECD - University of Zurich Expert Consultation "Protection of Children in a Connected World"*, https://one.oecd.org/document/DSTI/CDEP/SPDE(2019)3/en/pdf. [23]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [18]

OECD (2019), *The impact of digital government on citizen well-being*, https://doi.org/10.1787/24bac82f-en. [21]

OECD (2016), "Recommendation on Health Data Governance", https://www.oecd.org/els/health-systems/health-data-governance.htm#:~:text=The%20Recommendation%20calls%20upon%20countries,which%20there%20is%20a%20public. [28]

OECD (2014), *Recommendation of the OECD Council on Digital Government Strategies*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406. [94]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [17]

OECD (2011), *Guidelines for Multinational Entreprises*, https://mneguidelines.oecd.org/mneguidelines/. [120]

Office of the United Nations High Commissioner for Human Rights (2022), *What are human rights?*, https://www.ohchr.org/en/what-are-human-rights#:~:text=Human%20rights%20are%20inalienable.,by%20a%20court%20of%20law. [7]

Office of the United Nations High Commissioner for Human Rights (2021), *B-Tech Project "OHCHR and business and human rights"*, https://www.ohchr.org/en/business-and-human-rights/b-tech-project. [119]

Office of the United Nations High Commissioner for Human Rights (2018), *Report of the United Nations High Commissioner for Human Rights, on The Right to Privacy in the Digital Age A/HRC/39/39*, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf. [109]

OSCE (2019), *Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade*, https://www.osce.org/files/f/documents/9/c/425282.pdf. [85]

Psaila, S. (2011), *Right to access the Internet: the countries and the laws that proclaim it*, https://www.diplomacy.edu/blog/right-to-access-the-internet-countries-and-laws-proclaim-it/?nowprocket=1. [91]

Seibert-Fohr, A. (2018), *Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy*, https://ssrn.com/abstract=3168711. [108]

Shadmy and Shany (2021), *Protection Gaps in Public Law Governing Cyberspace: Israel's High Court's Decision on Government-Initiated Takedown Requests*, https://www.lawfareblog.com/protection-gaps-public-law-governing-cyberspace-israels-high-courts-decision-government-initiated. [45]

Shadmy, T. (2022), "Content Traffic Regulation: A Democratic Framework for Addressing Misinformation", *Jurimetrics*, Vol. 63/1, https://ssrn.com/abstract=4203322. [34]

Sutto, M. (2019), *Human Rights evolution, a brief history*, https://www.coespu.org/articles/human-rights-evolution-brief-history#:~:text=The%20origins%20of%20Human,religion%2C%20and%20established%20racial%20equality. [4]

Suzor, N. and R. Gillett (2022), *Self-Regulation and Discretion*, https://link.springer.com/chapter/10.1007/978-3-030-95220-4_13. [64]

The White House (2022), *What is the Blueprint for an AI Bill of Rights?*, http://whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/. [105]

UN General Assembly (1966), *ICCPR*, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. [30]

UN Group of Governmental Experts (GGE) (2021), *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, https://undocs.org/en/A/76/50. [111]

UN Human Rights Council (2018), *Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar*. [36]

UN Human Rights Office (2022), *What are human rights?*, https://www.ohchr.org/en/what-are-human-rights. [1]

UN Human Rights Office (2011), *UN Guiding Principles on Business and Human Rights*, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf. [16]

UN Special Rapporteur on Minority Issues (2021), *Report on the widespread targeting of minorities through hate speech in social media*. [10]

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2021), *Disinformation and freedom of opinion and expression*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/085/64/PDF/G2108564.pdf?OpenElement. [31]

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2017), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, https://www.ohchr.org/en/documents/thematic-reports/ahrc3522-report-special-rapporteur-promotion-and-protection-right. [73]

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2016), *Promotion and protection of the right to freedom of opinion and expression*, https://digitallibrary.un.org/record/844396?ln=fr. [72]

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf. [87]

UN Special Rapporteur on the right to privacy (2018), *Right to privacy (A/73/438)*, https://undocs.org/A/HRC/37/62. [80]

UNDP (2021), *The evolving digital divide*, https://www.undp.org/blog/evolving-digital-divide. [88]

UNESCO (2022), *UNESCO reaffirms need for Internet Universality, amid intensified threats*, https://www.unesco.org/en/articles/unesco-reaffirms-need-internet-universality-amid-intensified-threats. [89]

United Nations (2019), *United Nations Strategy and Plan of Action on Hate Speech*, https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdf. [123]

United Nations (1948), *Universal Declaration of Human Rights*, https://www.un.org/en/about-us/universal-declaration-of-human-rights. [6]

United Nations (1945), *UN Charter*, https://www.un.org/en/about-us/un-charter/full-text. [5]

United Nations (n.d.), *High-Level-Panel for Digital Cooperation Launches Report & Recommendations For Building an Inclusive Digital Futire*, https://www.un.org/techenvoy/news/HLP%20report%20launch. [113]

United Nations General Assembly (2016), *Resolution on the Right to Privacy in the Digital Age (A/RES/71/199)*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/455/32/PDF/N1645532.pdf?OpenElement. [127]

United Nations General Assembly (2013), *Resolution on the right to privacy in the digital age (A/RES/68/167)*, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F68%2F167&Language=E&DeviceType=Desktop&LangRequested=False. [2]

United Nations Human Rights Committee (2019), *Concluding observations on Nigeria in the absence of its second periodic report*, https://www.ohchr.org/en/documents/concluding-observations/ccprcngaco2-human-rights-committee-concluding-observations. [110]

United Nations Human Rights Council (2016), *The promotion, protection and enjoyment of human rights on the Internet (A/HRC/32/L.20)*, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/L.20. [126]

United Nations Human Rights Council (2014), *The promotion, protection and enjoyment of human rights on the Internet (A/HRC/RES/26/13)*, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F26%2F13&Language=E&DeviceType=Desktop&LangRequested=False. [125]

United Nations Human Rights Council (2012), *The promotion, protection and enjoyment of human rights on the Internet (A/HRC/20/8)*, https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/20/8. [107]

United Nations Special Rapporteur on Freedom of Opinion and Expression (2019), *Thematic report on online "hate speech" (A/74/486)*, https://www.ohchr.org/en/documents/thematic-reports/a74486-report-online-hate-speech. [43]

United Nations, Human Rights Committee (1988), *General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, https://www.refworld.org/docid/453883f922.html. [75]

Van der Vlies, R. (2020), "Digital strategies in education across OECD countries: Exploring education policies on digital technologies", *OECD Education Working Papers*, No. 226, OECD Publishing, Paris, https://doi.org/10.1787/33dd4c26-en. [27]

West, D. (2016), *Digital environment shutdowns cost countries $2.4 billion last year*, https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf. [71]

Wong, W. (forthcoming), *We, the data (working title)*, MIT Press. [40]

World Summit on the Information Society Forum (2003), *Declaration of Principles: Building the Information Society: a global challenge in the new Millennium*, https://www.itu.int/net/wsis/docs/geneva/official/dop.html. [114]

Zuboff, S. (2019), *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. [77]

Notes

[1] The explanation of rights within this paragraph should be read as a baseline definition of rights and does not seek to provide a comprehensive definition of rights, in general or in the context of this paper. This paper looks at a broad concept of rights, considering how the unique characteristics of the digital environment and data ecosystem have led to new concerns that human rights vocabulary may not accurately reflect.

[2] See for example article 19 of the International Covenant on Civil and Political Rights (UN General Assembly, 1966[30]).

[3] The discussion on conflict of rights in this paragraph is included to provide a basic overview of the conflict of rights. It does not seek to comprehensively address the conflict of rights within the complexities of the digital environment, but rather provide a starting point for the discussion to follow in this paper.

[4] These are OECD definitions, and do not intend to reflect definitions within individual legal systems.

[5] See, for example, the UN Strategy and Plan of Action on Hate Speech, which discusses the prohibition under international law on hate speech, which amounts to the incitement to discrimination (United Nations, 2019[123]).

[6] In certain laws and academic writing, this is called “revenge porn”. This paper uses the term “image-based abuse” considering concerns that such terminology is a misnomer given that the spreading of such content is often neither revenge nor pornographic (Australian eSafety Commissioner, n.d.[124]).

[7] Other relevant laws include: France’s “Fighting hate on the Internet” law, Israel’s Bill for the Prevention of Offenses through Internet (Content Removal), Austria’s Communication Platform Act (KoPlG), and Australia’s Online Safety Act.

[8] Empirical data on national policies in OECD countries is based on a sample of openly available material. A sound comparative mapping of national analyses would require more comprehensive data, including input from countries.

[9] This section sets out only initiatives that deal specifically with rights in the digital age, and therefore does not cover (often longstanding) laws and policies that address stand-alone legal questions that are also the subject of individual rights, and which digital transformation has impacted (e.g. privacy, health, education).

[10] In addition to these initiatives, Korea expects to introduce a Bill of Digital Rights in 2023 (Ministry of Science and ICT, Republic of Korea, 2022[122]).

[11]See for example the 2014 and 2016 HRC Resolutions on the promotion, protection and enjoyment of

human rights on the Internet (United Nations Human Rights Council, 2014[125]) (United Nations Human Rights Council, 2016[126]); and the UNGA 2013 and 2016 resolutions on the Right to Privacy in the Digital Age (United Nations General Assembly, 2013[2]) (United Nations General Assembly, 2016[127]).

[12] See also Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (the Police Directive). The Police Directive addresses law enforcement access to personal data, and the protection of the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.