Digital
Cooperation
Organization

DIGITAL RIGHTS

POLICY PAPER

2024

DOCUMENT DISCLAIMER

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, the DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. The DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

The DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between the DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of the DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall the DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining the DCO's consent or shall provide a reference to the DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

TABLE OF CONTENTS

EXECUTIVE **SUMMARY**

EXECUTIVE SUMMARY

This policy paper contributes to the promotion, safeguarding, and enhancement of digital rights within the context of fostering an inclusive, human-centric, and sustainable digital economy across the Digital Cooperation Organization's (DCO) Member States and beyond. It begins by contextualizing the significance of digital rights in the digital economy, along with the global and regional approaches that have been adopted and advocated. To achieve this, the paper identifies actions being taken by international organizations, supranational and regional entities, and countries within and outside the DCO membership.

The paper delves into the significant challenges currently facing digital rights and identifies specific initiatives being pursued globally to address them. It subsequently identifies and characterizes the digital rights deemed most pertinent within the context of DCO. Furthermore, the paper presents policy recommendations aimed at promoting, safeguarding, and enhancing these digital rights. The following list outlines eight digital rights that are particularly pertinent in the context of DCO, summarizing the paper's policy recommendations aimed at addressing these rights. :

Right to protection against online misinformation

- Apply advertising regulations like those outlined in the Audiovisual Media Services Directive (European Law) to the online sphere;
- Create a coalition of trusted media entities committed to collaborating on fact-checking and verifying authenticity and credibility of information.

Right to digital literacy

- Establish national/regional digital literacy strategies with robust educational components to empower more citizens to engage meaningfully online;
- Enhance and advocate for programs aimed at cultivating digital literacy skills.

Online Privacy protection

- Where missing, create regulatory bodies (at national or regional level) dedicated to enforcing privacy protection, and equip them with the necessary governance structure, resources, and technical proficiency to carry out their responsibilities effectively;
- Where missing, develop national privacy strategies, and ensure their alignment with existing and emerging strategies in the interconnected domains (e.g., with the national cybersecurity strategies);
- Establish certifications programs focused on data protection and privacy, alongside specialized educational offerings and professional development services.

Right to digital security and safety

- Acknowledge the critical need to support vulnerable and marginalized communities in exercising their rights in the digital realm, emphasizing the protection of children's safety and online privacy.
- Develop national cybersecurity strategies, ensuring their alignment with existing and new strategies in related domains, such as online privacy protection.
- Establish cybersecurity observatories to monitor the national cybersecurity landscape, encompassing its various components.
- Promote and acknowledge collaborative efforts involving multiple stakeholders to develop unified frameworks, systems, and protocols that are standardized across borders while respecting national sovereignty.

Right to personal digital identity

- Develop and deploy digital identity systems tailored to the requirements of users and service providers, while considering the national contexts, including digital readiness and ongoing digital identity initiatives;
- Ensure that policies and legal frameworks governing the design, development, and implementation of digital identity systems prioritize transparency, accountability, and alignment with user needs and expectations. This should be achieved through active engagement and participation of stakeholders;
- Establish interoperability among various national digital ID systems, thereby facilitating a seamless cross-border digital economy.

Protection against Algorithmic Bias

- Design and implement ethical governance standards for the responsible development, deployment, and use of AI.
- Conduct a comprehensive review and adjustment of current policy and regulatory frameworks concerning the AI systems. This process should include an assessment of existing laws, regulations, and guidelines to ensure they remain relevant and effective in addressing the evolving challenges and opportunities presented by AI technologies.
- Develop robust assessment mechanisms that can effectively evaluate the ethical, legal, and societal implications of AI systems, promoting transparency, accountability, and responsible innovation in the AI ecosystem.

RESEARCH METHODOLOGY

For this policy paper's development, a preliminary analysis of the reality, trends, and key challenges and initiatives worldwide in digital rights was conducted. Following this initial research, secondary research was carried out over the subsequent months.

During this period, the DCO conducted three global roundtables:

- **Roundtable in Riyadh – September 19, 2023**
- **Roundtable in Cape Town – November 15, 2023**
- **Roundtable in Geneva – December 7, 2023**

For each of these meetings, research was conducted with a special focus on the geographical areas where the roundtables took place: the Middle East, Africa, and Europe. Following these roundtables, surveys were distributed to the participants, and the results were incorporated into this policy paper.

Following this, a comprehensive analysis was conducted on all documentation, research findings, contributions from roundtables and meetings, and insights from the DCO. Moreover, a virtual discussion session on digital rights was held in January 2024 to present and discuss preliminary policy recommendations.

1 INTRODUCTION

INTRODUCTION

In the modern digital era, the importance and pertinence of digital rights cannot be overstated, given the central role technology plays in diverse facets of our lives. Digital rights constitute the safeguards and entitlements that individuals should have in the digital domain.

Digital rights are indispensable today. The extent to which technology permeates our lives presents a complex challenge to rights as we understand them. Ensuring that technology serves people and acts as a catalyst for further economic and social development while safeguarding essential human rights is crucial to a sustainable digital economy.

Digital Rights are central to the Digital Cooperation Organization's (DCO) vision of a prosperous global digital economy. DCO's Strategic Roadmap 2030 envisages DCO to be an 'advocate' in promoting effective policies for digital rights across its Member States and beyond. DCO's 'Flagship Initiative: DCO Digital for Good' has an emphasis on "extending Human Rights protection to the digital space, promoting an inclusive, safe, and ethical Digital Economy".

Furthermore, DCO's 2030 Roadmap identifies key challenges related to online harm, misinformation, data privacy, and AI bias that must be addressed to ensure user security and foster trust in digital technologies.

The solutions to the outlined issues are also aligned with United Nations' Sustainable Development Goals (SDGs). In specific goal 17 states, "*through cooperation, removing barriers to the flow of data and digital workers, aligning regulations on privacy and digital rights, and combining research capabilities to foster innovation would enable significant progress towards shared prosperity for all*". This is in direct alignment with the DCO's 2030 vision.

Moreover, numerous SDGs are intricately linked to digital rights, extending beyond the aforementioned Goal 17. For instance, Goal 4 - Quality Education which seeks to substantially enhance the skills of youth and adults encompassing technical and vocational expertise, for employment, decent jobs, and entrepreneurship. In the digital era, this necessarily involves fostering digital literacy. Similarly, Goal 9 - Industry, Innovation, and Infrastructure, which centers on a substantial increase in access to information and communications technology (ICT), along with the aspiration to provide universal and affordable Internet access in the least developed countries.

Digital rights undeniably occupy a prominent place on the global digital economy agenda.

The aim of this policy paper is to define digital rights, identify globally recognized digital rights, examine the approaches being pursued worldwide while simultaneously contextualizing the digital rights space within DCO Member States. The report concludes with policy recommendations that could help foster the digital economy, safeguard rights, and promote inclusion and human development.

2

DIGITAL RIGHTS OVERVIEW AND **GLOBAL APPROACHES**

DIGITAL RIGHTS – OVERVIEW AND GLOBAL APPROACHES

a) What are digital rights?

Digital rights encompass the fundamental liberties and protections individuals are entitled to in the digital age. The concept stands on the principles of an open and diverse online environment that is free from harm and discrimination. Digital rights have been understood as an extension of the broader human rights set out in the Universal Declaration of Human Rights [1] by the United Nations, as applied to the online world. In 2012, the United Nations' Human Rights Council [2] declared digital rights as human rights and affirmed that the same rights that people have offline must also be protected online. Given the cross-cutting nature of digital rights on a global scale, the involvement of multiple stakeholders is vital. States bear the responsibility of ensuring the protection of individuals' human rights within their respective jurisdictions. Nonetheless, the digital environment extends across numerous legal jurisdictions, involving policymakers, decision-makers, and subject matter experts (SMEs) from diverse sectors who share in the responsibility. Furthermore, private entities such as digital platforms play a significant role in enabling individuals to practically exercise their rights in the digital realm. As per the UN Guiding Principles on Business and Human Rights[3], these entities are also accountable for upholding human rights within their operations.

A crucial aspect of digital rights revolves around rights concerning the utilization of emerging technologies. These encompass novel rights linked to the application of such technologies. Examples of this include the right to personal data protection, digital inclusion, and digital literacy.

Hence, digital rights can potentially be categorized into two distinct groups:

1. **Human rights applied in the digital realm** – defining rights that are available to users both online and offline. As mentioned earlier, examples include the right to information, the right to privacy, education, and literacy. These rights deserve recognition and protection both offline and online.

2. **Rights specific to the digital realm** – i.e., the rights solely focused on the use of digital technologies and the internet. Few examples of these rights include the right to personal data protection, which involves control and self-determination over personal information collected, stored, and processed by third parties on the internet; the right to digital inclusion, ensuring that everyone has access to digital technologies and their benefits; and the right to digital education and citizenship, involving empowering people for the critical and responsible use of digital technologies.

b) Why are digital rights crucial to the digital economy?

Technology has become indispensable in shaping how societies operate and how people interact. Business interactions and transactions increasingly rely on the digital technologies across the entire value chain. Moreover, individuals are constantly immersed in technology, from the moment they wake up until they go to bed. The pervasive integration of technology into people's daily lives underscores the paramount importance of digital rights in shaping a sustainable and inclusive digital economy. Similarly, as technological advances become increasingly interconnected, and as businesses collect vast amounts of personal data online, the integration of data protection and privacy into the digital rights have become immensely crucial. This should be viewed from a dual perspective:

1. First, from a proactive standpoint, emphasizing the importance of data protection and privacy in the context of a rapidly growing digital economy.

2. Second, from a risk-oriented perspective, considering the heightened risk of cyberattacks and breach of digital security that can cause significant harm.

Increased proliferation of digital technologies brings vulnerabilities owing to occurrences of cyberattacks and security breaches. These are threats to citizens, governments, businesses, trade, and national economies. Safeguarding vulnerable people, especially children, is of paramount concern.

Numerous studies have consistently emphasized how digital rights play a pivotal role in fostering an inclusive, secure, and innovative digital economy that delivers benefits to individuals, businesses, and societies worldwide.

In 2016, a World Bank Report[4] analyzed the impact of the internet and new technologies on the global economy and economic development. The report emphasized the key role of digital rights such as privacy and security in translating this positive impact to the general population.

The following year, the OECD published a report[5] along the same lines, demonstrating the impact of digital transformation on economies and societies, highlighting the importance of digital rights such as privacy and consumer rights to enhance confidence in the digital economy. More recently, in another report[6] on rights in the digital age, the OECD reiterated the importance of digital rights for the digital economy.

Therefore, the significance of digital rights in the context of the digital economy cannot be overstated. Various digital rights, such as privacy and personal data protection, digital inclusion and digital literacy, digital safety and security, and IP protection play a pivotal role in shaping a thriving digital ecosystem.

Recognizing and upholding the digital rights not only ensures the protection of individuals in the digital sphere but also fosters an environment conducive to innovation, economic growth, and equitable participation in the evolving digital landscape. Embracing and championing digital rights is not just a matter of ethical consideration but a strategic imperative for the sustained prosperity of the digital economy on a global scale.

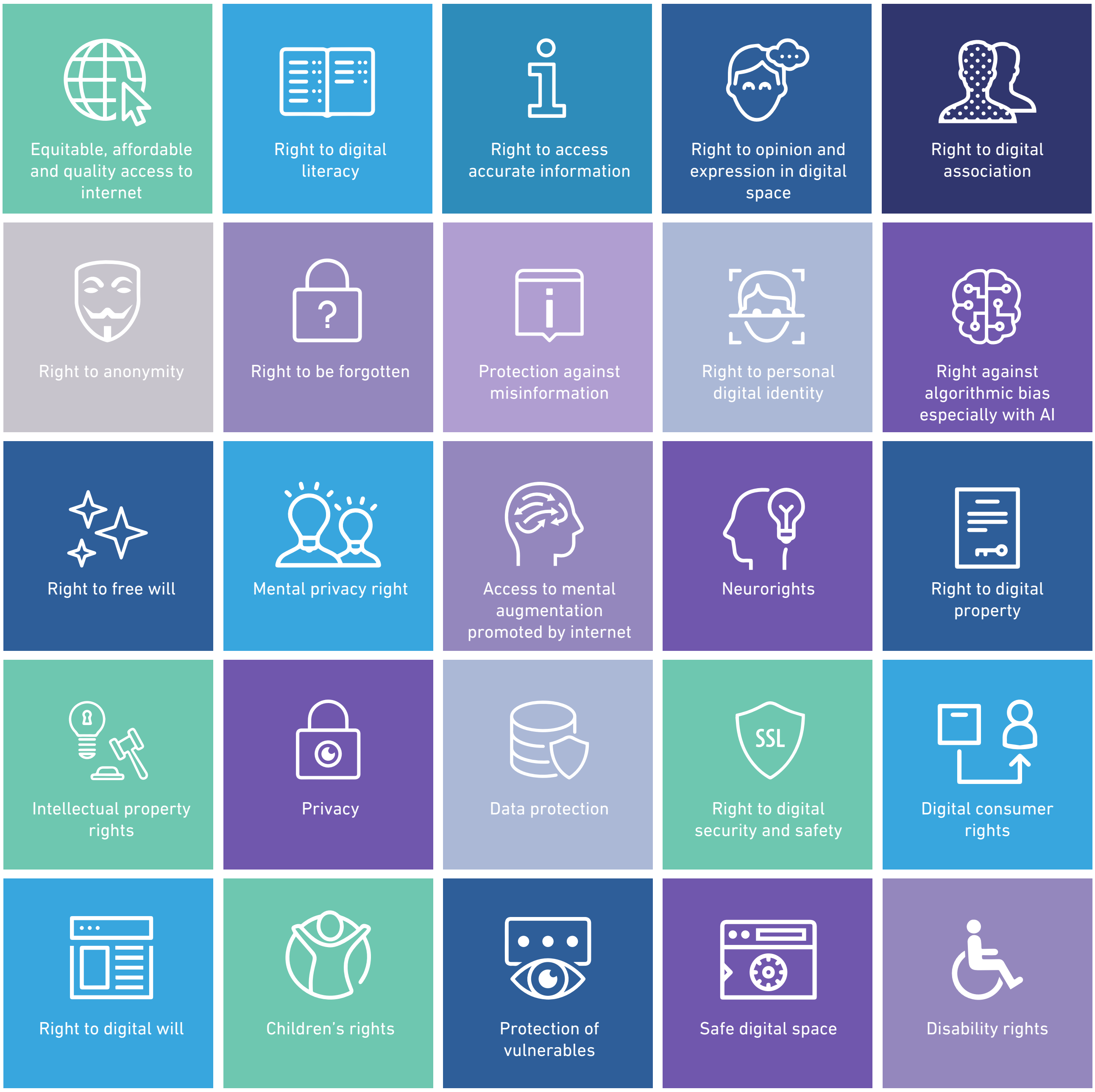
3

DIVERSE GLOBAL APPROACHES **TOWARD DIGITAL RIGHTS**

DIVERSE GLOBAL APPROACHES TOWARD DIGITAL RIGHTS

Consistently evolving, the realm of digital rights has witnessed numerous developments in recent years. On one hand, there is a list of rights globally adopted by countries or international, supranational, and regional organizations. On the other hand, the approach towards tackling specific digital rights has also varied significantly on the national and regional levels.

Globally, we have witnessed the acknowledgment of a significantly broad set of rights applied to digital space. Some of the rights that have been recognized span across diverse areas and domains, including:



Equitable, affordable and quality access to internet

Right to digital literacy

Right to access accurate information

Right to opinion and expression in digital space

Right to digital association

Right to anonymity

Right to be forgotten

Protection against misinformation

Right to personal digital identity

Right against algorithmic bias especially with AI

Right to free will

Mental privacy right

Access to mental augmentation promoted by internet

Neurorights

Right to digital property

Intellectual property rights

Privacy

Data protection

Right to digital security and safety

Digital consumer rights

Right to digital will

Children's rights

Protection of vulnerables

Safe digital space

Disability rights

Figure 1: Examples of globally acknowledged digital rights (non-exhaustive)

a) Global Approaches

The digital rights that have been recognized and expanded are very diverse, and so are the approaches that are adopted by countries and organizations towards addressing them. Below, we will attempt to capture the types of approaches that have been adopted by different jurisdictions to safeguard some of the key digital rights and will detail various options and initiatives that have been promoted worldwide.

Three broad global approaches, as categorized by the OECD[6], have been adopted:

1. Developing broad policy frameworks that attempt to cover digital rights holistically;
2. Defining new digital rights in specific domains, and mapping them against selected gaps, e.g., the need for algorithmic transparency and accountability for decisions made by Artificial Intelligence (AI); and
3. Prioritizing protection of human rights online in a comparable way as they are protected offline.

In the **first approach**, through which broad policy frameworks around digital rights have been developed, normative frameworks are created aiming to comprehensively encompass rights that are relevant to the digital space. The best example of this type of approach is the establishment of **digital rights charters**, whether binding or non-binding, that systematize a set of digital rights. Brazil, Italy, Spain, and Portugal are some of the countries that have followed this approach.

The **second approach**, in which new digital rights in specific domains are developed, aims to address rights in areas considered crucial. One such example is Chile's choice to include brain rights in its constitution, with the aim of protecting mental privacy, free will, and non-discrimination while accessing the neurotechnology.

The **third approach**, protecting digital rights similarly to how they are safeguarded offline, constitutes an extension of the protection of human rights that already existed, but now within the context of the digital space. One such example is bullying, criminalized in various jurisdictions, which has led to the creation of rights like condemning bullying done through online platforms.

Annexure A includes detailed examples of how different countries have applied the above approaches to address some of the crucial digital rights within their jurisdictions.

b)Role of Supranational Organizations and Multilateral Efforts

In support of the national efforts, supranational organizations play a pivotal role in setting standards, advocating for policies, and coordinating efforts to safeguard digital rights. Below are some examples of the multifaceted role that international organizations are playing in promoting and protecting digital rights, highlighting their initiatives, collaborations, and publications aimed at fostering a secure, inclusive, and rights-respecting digital environment on a global scale.

i. The United Nations

The United Nations has devoted significant attention to digital rights, notably through the United Nations Hub for Human Rights and Digital Technology [7]. This initiative emerged following the Secretary General's launch of two groundbreaking initiatives in 2020, namely, a Call to Action for Human Rights [8] and a Roadmap for Digital Cooperation [9], both crafted in response to the evolving digital era. This Hub compiles reports, analyses, and recommendations from United Nations human rights mechanisms aimed at addressing human rights challenges in the digital age. There are numerous United Nations publications [10] on these matters. Lately, the UN Digital Compact [11], regarding Digital Rights, has emphasized, for example, the need to developing solutions that involve greater guidance on the application of human rights standards in the digital age and addressing the gaps created by evolving digital technologies.

ii. Organization for Economic Co-operation and Development (OECD)

In a similar vein, the **OECD**, particularly through its Committee on Digital Economy Policy, focuses on promoting discussions and conducting research on digital rights. Through extensive research, analysis, and policy guidance, the organization has been playing an instrumental role in understanding the implications of digital transformation on our societies and economies. The OECD has developed crucial standards to assist countries in various facets of digital transformation, encompassing: the Recommendation on Broadband Connectivity [12], the Recommendation on Artificial Intelligence [13], the Recommendation on Children in the digital environment [14], the Recommendation on Enhancing Access to and Sharing of Data [15], the Recommendation on Digital Security of Critical Activities [16], the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [17] and an ongoing project to develop a Voluntary Transparency Reporting Framework for Terrorist and Violent Terrorist Content online [18].

iii. The European Union (EU)

The European Union (EU) is another example of a supranational organization focusing on digital rights. On 15 December 2022, the Presidents of the Council of the EU, the European Parliament, and the European Commission signed **the European Declaration on Digital Rights and Principles for the digital decade** [19]. It includes references to digital sovereignty in an open manner, respect for fundamental rights, the rule of law, inclusion, accessibility, equality, sustainability, resilience, security, improving the quality of life, the availability of services, and respect for everyone's rights and aspirations. As principles, this declaration is based on six main ideas:

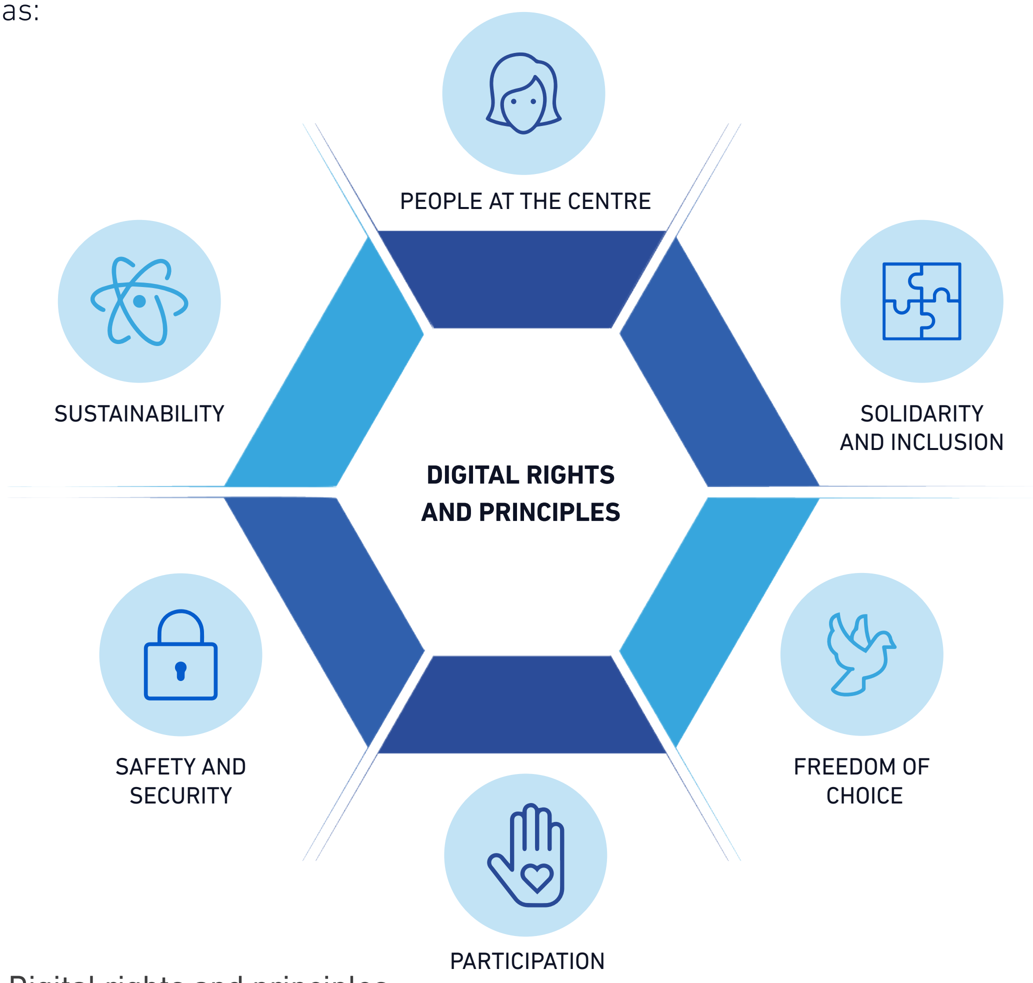


Figure 2: Digital rights and principles

The declaration finds its foundation in EU law, encompassing the Treaties, the Charter of Fundamental Rights [20], and the jurisprudence established by the EU Court of Justice. The Commission will oversee the advancement of the declaration's objectives and has offered relevant recommendations via an annual report [21] titled the 'State of the Digital Decade'.

Case Study

In the field of digital services, the European Union's important and recent legislative framework serves as an exemplar for any legislation or recommendations on digital rights. On September 15, 2020, the European Commission introduced the **Digital Services Act** (DSA) alongside its companion legislation, the Digital Market Act (DMA). The goal of the DSA is to safeguard the digital environment from the dissemination of illicit content and to guarantee the protection of users' fundamental rights. It adheres to the principle that activities deemed illegal offline must also be considered illegal online and will be applicable to all online intermediaries offering services within the EU. The DSA establishes a distinction between 'very large platforms,' those with over 45 million active users in the European Union, and other platforms. Its objective is to combat illegal content by simplifying the process of reporting and moderating such content on platforms. The Digital Services Act also requires the marketplaces to enhance their monitoring and identification of third-party vendors. Additionally, the regulation demands increased transparency from platforms concerning moderation practices, content recommendations, and advertising. Major platforms will undergo systemic risk analyses, independent audits, and will need to disclose their algorithms to the relevant regulatory authorities.

Regarding the regulation of artificial intelligence, the European Parliament recently announced what could be the world's first artificial intelligence (AI) regulatory framework. The central objective of this legislation, known as the **Artificial Intelligence Act** or AI Act, is to ensure the safe use of AI by incorporating appropriate human oversight. The legislation outlines key principles, including developing AI in a manner that aids and respects individuals, minimizes harm, adheres to high privacy and data protection standards, ensures transparency, and fosters equality. These objectives are integral to the new drafting, akin to the foundational principles of the **General Data Protection Regulation** (GDPR) [22].

AI systems, in the AI Act [23], are divided into four risk categories: **unacceptable** (e.g. classifying people based on behavior, socio-economic status or personal characteristics), **high** (e.g. AI systems that are used in products falling under the EU's product safety legislation), **limited** (e.g. AI systems with a risk of manipulation or deceit, and need transparency) and **minimal** (all other AI systems that do not fall under the above-mentioned categories, e.g. a spam filter). According to this legislation, certain AI systems would be prohibited altogether, whereas other types of AI would be permitted, but would be subject to several obligations regarding their development, placing on the market, and use. A list of prohibited practices encompasses all AI systems whose usage is deemed unacceptable, as they contradict EU values, especially by violating fundamental rights. These prohibitions extend to practices with a significant potential to manipulate individuals through subliminal techniques beyond their awareness or exploit vulnerabilities in specific groups such as children or persons with disabilities, leading to a material distortion of their behavior likely to cause psychological or physical harm to them or others. Furthermore, manipulative or exploitative practices targeting adults that could be facilitated by AI systems may fall under existing data protection, consumer protection, and digital service legislation. These regulations ensure that individuals are adequately informed and have the freedom to choose not to be subjected to profiling or other practices influencing their behavior. Specifically, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes is also prohibited, except under certain limited exceptions.

It is worth noting that the **General Data Protection Regulation** (GDPR) is considered the most stringent privacy and security law globally. Enacted by the European Union (EU), this regulation imposes obligations on organizations worldwide if they handle data related to individuals in the EU. Effective since May 25, 2018, the GDPR mandates severe fines for non-compliance with its privacy and security standards, with penalties potentially reaching tens of millions of Euros.

iv.Association of Southeast Asian Nations (ASEAN)

The definition of AI governance is intrinsically linked to digital rights. Indeed, the establishment of frameworks, regulations, and ethical guidelines to ensure responsible and fair use of artificial intelligence (AI) technologies enables the safeguarding and protection of individuals' digital rights. As AI systems become increasingly integrated into various aspects of society, including decision-making processes, the protection of digital rights becomes a critical consideration.

ASEAN which is a political and economic union of 10 Southeast Asian countries has recently initiated negotiations on the ASEAN Digital Economy Framework Agreement (DEFA) [24] in September 2023, marking what is aspired to be the world's first major region-wide digital economy agreement. One of the provisions of DEFA is AI Governance which focuses on the implementation of ethics and governance structure, cooperation on innovation and AI regulation, and harmonization of AI standards and governance. ASEAN's goal to establish itself as an independent and strong regional association is reflected in its intention to harmonize any applicable AI standards and governance approaches which are currently being adopted by ASEAN's Member States, for example, AI Verify toolkit by Singapore. This toolkit helps AI developers gain a better knowledge about their AI governance position and what they should change to achieve better AI governance.

v. Others

Currently, under discussion among **22 Ibero-American countries** is the creation of a digital rights charter [25]. The Ibero-American Summit, which convenes most Latin American heads of state, serves as the primary high-level political gathering in the region. The Ibero-American Charter of Digital Principles and Rights will be a non-binding instrument with voluntary adherence by the states. It aims to establish a regional framework that promotes the most up-to-date development of regulatory frameworks and serves as a compass for the development of national public policies, placing individuals at the center of digital transformation. The objective of this document is to be declaratory and non-binding. Its purpose is to advocate common principles for the relevant states to consider while adopting or adapting national legislation. It also guides the implementation of public policies concerning the protection of rights and the fulfillment of duties in digital environments. This document provides a framework for companies, civil society, and academia when developing and applying technologies, prioritizing people during digital transformation. The agreement received widespread consensus among the ICT ministries of the concerned countries.

vi.DCO

As expressed earlier, digital rights are at the heart of the DCO's agenda. DCO's Strategic Roadmap 2030 (the Roadmap) envisages DCO to be an 'advocate' in promoting effective policies for digital rights across its Member States and beyond. DCO's 'Flagship Initiative: DCO Digital for Good' has an emphasis on "extending Human Rights protection to the digital space, promoting an inclusive, safe, and ethical Digital Economy". In the Roadmap, the DCO has set itself a goal (Goal 3) to "foster an inclusive, human centric, and sustainable Digital Economy", and to achieve this goal, the DCO's objectives 3.1 and 3.2 emphasize the need of ensuring a 'safe digital space for children and the most vulnerable segments of the society', and to 'empower people by improving the quality, access, inclusiveness, and interoperability of digital goods and services'.

The Roadmap also identifies key challenges related to online harm, misinformation, data privacy, and AI bias that must be addressed to ensure user security and foster trust in digital technologies.

Furthermore, the DCO has been making ongoing efforts to promote digital rights by instigating global dialogues through global DSA roundtables and putting forward impactful and actionable recommendations through its publications.

c) DCO Member States' Positions on Digital Rights

In examining the contemporary landscape of digital rights protection within the DCO Member States, it becomes evident that the evolving digital ecosystem necessitates a comprehensive and coordinated approach. This section delves into the efforts towards preserving digital rights across the DCO Member States. By scrutinizing the diverse initiatives, policies, and laws, we aim to provide insights into the efforts made by the DCO Member States in protecting various digital rights, which demonstrates their interest in the subject.

The table below summarizes examples of some key initiatives implemented by the DCO Member States.

Tabe 1: Examples of initiatives across the DCO Member States to address Digital Rights

Member States	Initiatives	
	Bahrain	Laws related to data protection and cybersecurity
	Bangladesh	The New Cyber Security Act
	Cyprus	GDPR establishing comprehensive regulations for personal data processing
	Djibouti	Expansion of connectivity and broadening access to digital technologies
	The Gambia	Information and Communications Technology Agency Act
	Ghana	Digital Financial Services Policy
	Greece	The Law on Emerging Information Technology and Communication Technologies
	Jordan	Promotion of high level of internet penetration and enhancement of digital literacy and education
	Kuwait	Data privacy protection regulation

Morocco	Regulation for personal data protection
Nigeria	Digital rights legislation (Cybercrime Act, Communications Act, and Digital Rights and Freedoms Bill)
Oman	Comprehensive data protection law
Pakistan	Digital Gender Inclusion Strategy, along with 3 years implementation plan by Pakistan Telecommunication Authority (PTA) developed in partnership with UNESCO
Qatar	Personal Data Protection (DPL)
Rwanda	Child Online Protection Policy
Saudi Arabia	Personal Data Protection Law

Short of adopting specific digital rights charters, several DCO Member States have undertaken several initiatives within the realm of digital rights. Some examples of these initiatives are captured below:

Bahrain has enacted laws related to data protection and cybersecurity [26], and initiatives have been introduced to promote digital literacy and inclusion among its citizens.

The new Cyber Security Act was recently approved by the Parliament of **Bangladesh**. Its objective is to combat the misuse of information technology, which in some cases has endangered people's lives and property. The Cyber Security Act of 2023 [27] aims to ensure the safety of people from all forms of cyber abuse and risks.

Cyprus, as an EU member, adheres to the GDPR, implementing comprehensive regulations for personal data processing, including digital data protection.

Djibouti has invested in expanding connectivity and broadening access to digital technologies to improve its peoples' access to digital services.

In 2019, **The Gambia** introduced the Information and Communications Technology Agency Act [28], which tackled cybercrime and promoted optimal ICT use, along with infrastructure and service investment.

In 2020, **Ghana** launched the Digital Financial Services Policy [29], aimed at enhancing financial inclusion through digital platforms.

In March 2023, the Law on emerging information technology and communication technologies [30], strengthening digital governance and other provisions, entered into effect, following its passage on July 2022, by the Hellenic **(Greek)** Parliament. The Law outlines its aim to provide appropriate guarantees to ensure the rights of natural persons and legal entities, strengthening accountability and transparency in the use of artificial intelligence (AI) systems, and complementing the existing institutional framework for cybersecurity.

Jordan boasts a relatively high level of internet penetration, complemented by initiatives to foster digital inclusion. Efforts have been dedicated to enhancing digital literacy and education, ensuring citizens are well-informed about their digital rights.

Kuwait released the Data Privacy Protection Regulation in 2024 [31], outlining detailed guidelines for managing and processing data by telecommunications and information technology service providers.

Morocco has a national regulation for personal data protection [32].

Nigeria has enacted digital rights legislation[33], including the Cybercrime Act, Communications Act, and the Digital Rights and Freedoms Bill.

In 2022, **Oman** introduced its first comprehensive data protection law [34], encompassing 32 articles covering data protection principles, the obligation to appoint a Data Protection Officer ('DPO'), data subjects' rights, duties of data controllers and processors, and penalties for breaches.

Since 2022, the **Pakistan** Telecommunication Authority (PTA) has actively participated in the Multi-Advisory Board for UNESCO's Internet Universality Indicators Assessment in the country. Following the findings and feedback, UNESCO and PTA engaged in bilateral discussions to enhance collaboration, with a particular focus on gender inclusion and the utilization of ICTs. This has culminated into the release of the 'Digital Gender Inclusion Strategy'[35] in February 2024, aimed at advancing access to information via ICTs in Pakistan. This strategy, with its 3 years action plan, will provide guidance to policymakers and stakeholders, enabling them to enhance institutional frameworks for promoting access to information both online and offline while incorporating a gender-responsive approach.

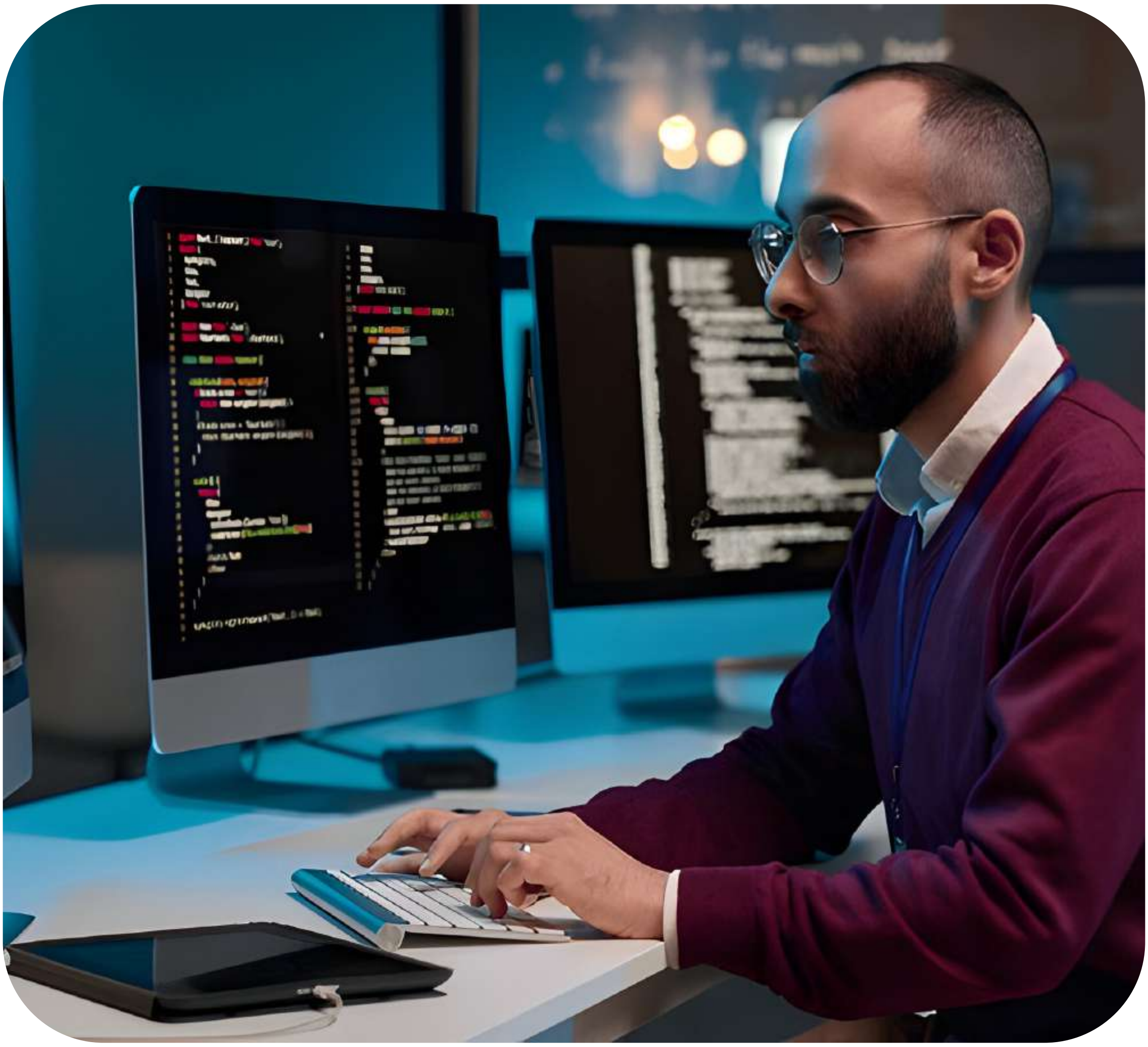
On December 29, 2016, **Qatar** enacted Law No. 13 of 2016 Concerning Personal Data Protection [36], commonly referred to as the DPL. This legislation safeguards individuals' right to the protection of their personal data. It establishes strict mandates for any entity handling personal data, emphasizing transparency in their practices. This transparency is ensured through various measures, including obtaining consent from the data subject, notifying the data subject, and reporting data breaches to the affected individuals, among other protective provisions.

Since 2016, **Rwanda** has implemented legislation targeting cybercrime and the prevention of electronic crimes. Having come into effect in July 2019, the Rwanda Child Online Protection Policy [37] is a response to the risks of minors being exposed to unsuitable content on the internet. The Policy is designed to mitigate against the risks and harms of the internet, providing a framework that addresses children's needs and upholds their rights while enabling them to safely and confidently navigate the digital environment.

Regarding **Saudi Arabia**, the Smart Government Strategy[38] addresses digitization, raising citizens' awareness, access, and utilization of Smart Government services. In 2023, updates were made to the Personal Data Protection Law[39], enhancing personal data safeguarding in alignment with international standards amid efforts to bolster the country's digital economy.

This array of initiatives and legislations adopted by, and under way in the DCO Member States demonstrate their serious concern towards addressing key challenges that are emerging in the domain of digital rights across the world.

As mentioned earlier, more examples on digital rights initiatives from several other countries are included at **Annexure A**.



4

KEY CHALLENGES FACING THE DIGITAL RIGHTS AND **APPROACHES TOWARDS ADDRESSING THEM**

KEY CHALLENGES FACING THE DIGITAL RIGHTS AND APPROACHES TOWARDS ADDRESSING THEM

The challenges in the field of digital rights are numerous, given the impact and significance they hold in today's world, particularly for the digital economy. Social and human development is now intricately linked to technologies that constantly undergo advancements.

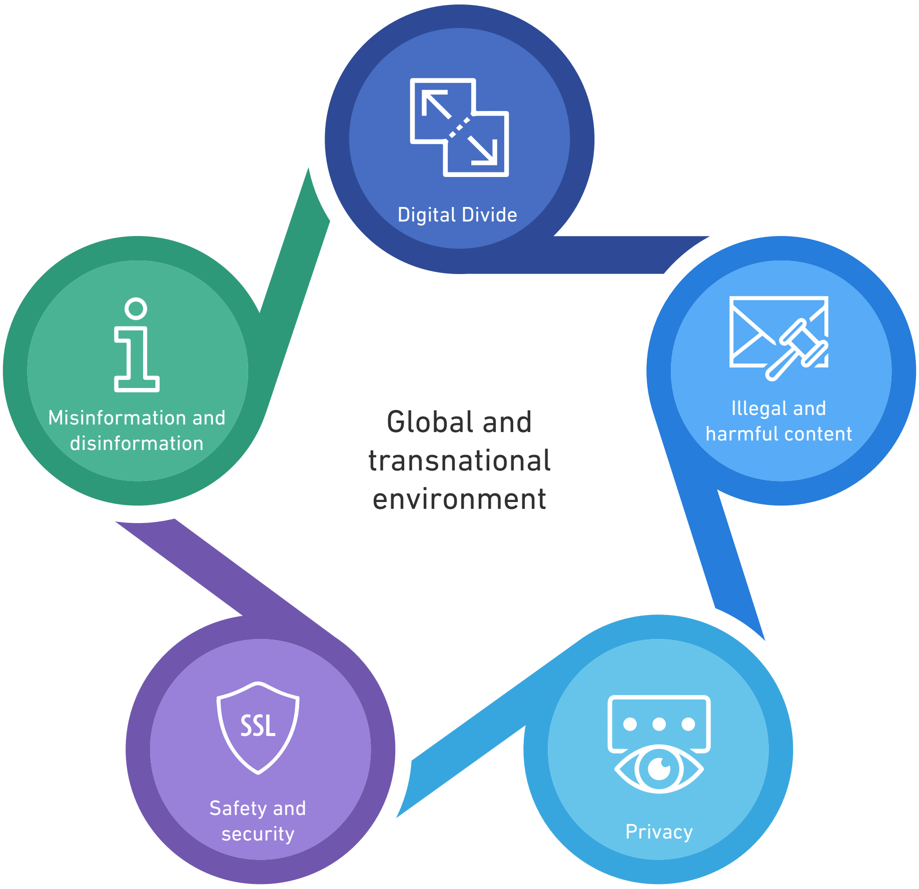

Digital Divide
Illegal and harmful content
Privacy
SSL
Safety and security
Misinformation and disinformation
Global and transnational environment

Figure 3: Key Challenges Facing Digital Rights

From a multitude of **challenges**, we attempt to categorize the key challenges that need to be overcome through promoting and advancing the digital rights into **five main categories namely**: digital divide; misinformation and disinformation; illegal and harmful content; safety and security; and privacy.

These challenges are shaped by the global and transnational nature of digital space. It is important to note that despite this categorization into five major types, each of the digital rights aims to address more than one of them, thereby fitting into more than one challenge. For example, children's rights in the online world seek to address the challenges of digital divide, illegal and harmful content, privacy, safety and security, and misinformation and disinformation.

a) Digital Divide

Accessibility to technological advancements is one of the primary concerns regarding digital rights. Despite advancements, a significant portion of the population still lacks internet connectivity, as highlighted in the Digital Global Overview report 2023[40].

Further, digital literacy skills, as an important component of digital rights, are especially important amongst vulnerable groups, particularly children. The ability to use new technologies effectively, identify their challenges, and fully leveraging their benefits is a dimension to consider and is a global concern.

It is crucial to understand how countries globally are addressing the identified challenges. We present here a few examples from the numerous programs, initiatives, and strategies developed to address the digital divide.

i. Globally

Regarding inclusion in the digital arena, various strategies are being pursued worldwide. The focus has been on enhancing access and promoting awareness and responsibility in new technologies. The information society and digital economy necessitates a dedicated focus on inclusivity as a fundamental challenge .

Among the several strategies being implemented, expansion of internet access stands out. In this domain, there are investments in infrastructure, with a particular emphasis on rural or remote areas. One of the most significant recent contributions in this field is the Roadmap for Digital Cooperation by the Secretary-General of the United Nations [41] which established a set of initiatives to promote discussion and political commitments on these matters, exemplified by activities such as roundtables [42], involving participants from around the world.

Digital literacy programs, state subsidies and incentives, are some of the initiatives that are developed to promote digital inclusion. For instance, some countries have introduced social internet service access tariffs (e.g., Brazil, Argentina, France, Portugal) to facilitate affordable internet access.

In the realm of inclusion, countries have been focusing on entrepreneurship and innovation to enhance internet access for vulnerable or underserved populations. The **United States** has the 'Connect America Fund'[43] program by the Federal Communications Commission (FCC), that is aimed at expanding broadband access in rural and hard-to-reach areas. **India** launched the 'BharatNet'[44] program to provide high-speed fiber optic connectivity to remote villages nationwide. The **German** government introduced the 'Digitale Dörfer'[45] (Digital Villages) program to enhance digital infrastructure in rural areas providing high-speed internet access. Similarly, the **United Kingdom's** 'Gigabit Broadband Voucher Scheme'[46] provides subsidies to businesses and residences to install high-speed internet connections.

ii. Examples from the DCO Member States

All the DCO Member States are putting in efforts to bridge the digital divide. Some examples are as follows:

The Kingdom of **Bahrain** has undertaken numerous initiatives to ensure that the internet and public data are open and accessible to all. Bahrain's policies and strategies focus on inclusive programs to support citizen participation. As part of its eGovernment National Strategy[47], the Information and eGovernment Authority (iGA) has implemented a program aimed at enhancing citizens' computer knowledge. Bahrain's eParticipation [48] policy emphasizes inclusivity by creating improved opportunities and resources, amplifying voices, and respecting the rights of individuals who are potentially disadvantaged based on age, gender, disability, race, ethnicity, origin, religion, or economic status.

Qatar has been actively promoting digital inclusion through its Digital Society and Digital Competencies department (integrated into the Ministry of Information and Communication Technology (MCIT)). This department is engaged in ongoing projects that focus on supporting various segments of the population, including Qatari women, expatriate laborers, individuals with disabilities, and residents of remote areas. Additionally, there are plans in place to promote intergenerational learning by nurturing Qatari youth as champions in the field of Information and Communication Technology (ICT).

In 2021, the World Bank approved a credit of US$10 million to support **Djibouti**'s endeavors in accelerating digital transformation and fostering a more inclusive digital economy. To realize Djibouti's ambition in becoming a regional digital hub, there needs a significant improvement in the country's connectivity infrastructure. The newly launched Digital Foundations Project seeks to address this need by ensuring wider access to quality and affordable internet for both citizens and businesses. The project aims to promote the uptake of digital skills and services. Aligned with Djibouti's Vision 2035 [49] and the new Country Partnership Framework [50], this initiative recognizes the pivotal role of ICT in driving economic growth.

Kuwait has been actively forging partnerships to enhance digital inclusion. Recently, Kuwait took a significant leap towards digital inclusivity by collaborating with Starlink, a satellite internet constellation developed by SpaceX. This partnership holds the promise of narrowing the digital divide within Kuwait. Presently, certain areas in the country lack access to reliable internet connections, particularly in remote and rural regions. This limited connectivity obstructs educational opportunities, hampers economic growth, and restricts access to essential services. Through this collaboration with Starlink, Kuwait aims to surmount these challenges, ensuring every citizen has equitable access to the digital world.

b) Misinformation & Disinformation

Disinformation denotes the deliberate dissemination or sharing of verifiably false, misleading, manipulated, created, or fabricated information. Its primary objective is to inflict harm upon the reputation of, or to harass individuals, driven by political, personal, or financial motives. Disinformation often neglects to include alternative perspectives, either by intentionally ignoring them or by providing inadequate coverage and space. On the other hand, misinformation refers to the unintentional dissemination or sharing of verifiably false content or information.

Fueled by social media, misinformation and disinformation has emerged as a major challenge of the digital era, giving rise to critical issues. The spread of false or misleading information through social networks and communication platforms poses significant threats to societies worldwide, sometimes resulting in real world harm. While the problem of misinformation is not new, the ease with which information can now be disseminated to large audiences, often anonymously and without verification, has amplified the risks, making it imperative to address the issue urgently.

During the COVID-19 pandemic, as efforts were made to address the public health emergency, misinformation and disinformation proliferated, contradicting scientific evidence and facts, thereby jeopardizing the health and safety of individuals. Four studies [51] looked at the proportion of health misinformation on social media and found that it reached up to 51% in posts associated with vaccines, up to 28.8% in posts associated with COVID-19, and up to 60% in posts related to pandemics. Among YouTube videos about emerging infectious diseases, 20–30% were found to contain inaccurate or misleading information [51].

The importance of addressing misinformation has been a global topic of concern over the past years. Some examples of how the misinformation & disinformation challenge is being addressed globally, are mentioned below.

i. Globally

From the EU's Code of Practice on Disinformation[52] to national-level legislations like Singapore's Protection from Online Falsehoods and Manipulation Act [53], and initiatives such as the Verified Campaign [54] by the United Nations and Purpose (a global social mobilization organization), numerous entities are actively working to counter the dangers and threats posed by misinformation.

In 2017, the **European Union** established a high-level group to assist in crafting policies to combat the growing issue of misinformation in Europe. In 2018, the group published its final report on fake news and disinformation [55], drawing on insights from experts worldwide who gathered over several weeks to advise the EU on how to tackle misinformation.

This report recommended responses based on **five pillars:**

- Enhance **transparency** of online news, involving appropriate and privacy-compliant sharing of data about the systems enabling their circulation online.
- Promote **media and information literacy** to counter disinformation and assist users in navigating the digital media environment.
- Develop **tools to empower users** and journalists to combat disinformation and encourage positive engagement with rapidly evolving information technologies.
- Safeguard the **diversity and sustainability** of the **European news media ecosystem.**
- Promote **ongoing research on the impact of disinformation** in Europe to assess measures taken by different actors and continually adjust necessary responses.

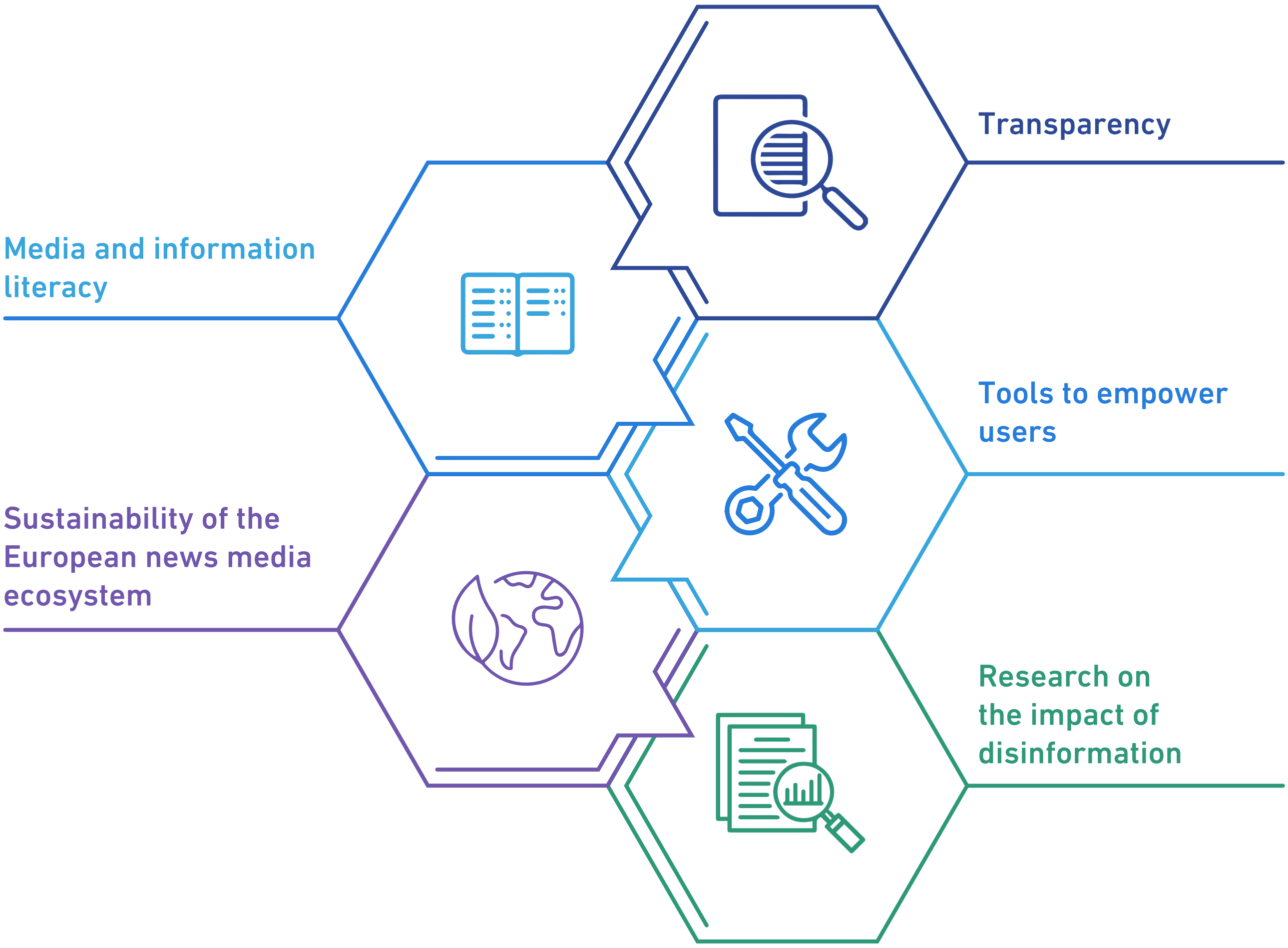

Transparency
Media and information literacy
Tools to empower users
Sustainability of the European news media ecosystem
Research on the impact of disinformation

Figure 4: Five pillars of EU approach to disinformation

The **Council of Europe** also produces reports in this domain, offering recommendations to policymakers.

In June 2019, **Mexico's** President inaugurated Verificado [56], a fact-checking initiative, integrated into the government's news agency Notimex [57].

In **Argentina**, the Public Defender's Office established the Observatory of Disinformation and Symbolic Violence on Digital Media and Platforms (NODIO) [58] in October 2020. This initiative aims to detect, verify, identify, and counter malicious news.

Brazil has been discussing the Brazilian Internet Freedom, Responsibility, and Transparency Law [59] for the past three years. Advocates view this legislation as a chance to curtail the harmful influence of major social media platforms in Brazil, making them responsible for the unrestricted dissemination of content from which they profit.

In **Australia**, there is an ongoing discussion about a law aimed at combating misinformation and disinformation. The proposed Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 [60] intends to amend the Broadcasting Services Act 1992 and other relevant legislation, granting new powers to tackle online misinformation and disinformation. Under this Bill, the Australian Communications and Media Authority (ACMA) would be empowered with enforcement capabilities, including: the authority to establish digital platform rules regarding records, including providing these records to the regulator; information and document gathering powers with which to compel digital platform providers, exercised as needed; access to public information collected under the information gathering powers; establishment of enforceable misinformation codes and standards to govern the digital platform industry's practices; the authority to request an industry body to develop, modify, or deregister an industry standard; and inclusion of electoral and referendum content within the scope of information powers (though without imposing obligations on political parties regarding misleading and deceptive conduct). It is important to note that private user messages will not fall under the purview of these powers.

ii. Examples from the DCO Member States

As noter earlier, misinformation and fake news emerged as significant challenges worldwide during the COVID-19 pandemic. To combat this issue in **Morocco**, the government council approved Law 22-20, addressing the use of social media, open broadcast networks, and similar platforms [61]. Morocco's legal framework previously lacked specific laws to deter crimes committed through social media, such as spreading false news and blackmail. The new law serves multiple purposes, including safeguarding digital communication freedom while documenting various forms of online crimes, especially those endangering public security or individuals. Additionally, the legislation focuses on crimes involving minors, outlines procedures for handling illicit electronic content, and defines sanctions against cybercrime.

In August 2023, **Pakistan** introduced legislation to tackle fake news. The Pakistan Electronic Media and Regulatory Authority (PEMRA) Amendment Bill 2023 [62] includes clear definitions for "disinformation" ("*disinformation means verifiable false, misleading manipulated, created or fabricated information which is disseminated or shared with the intention to cause harm to the reputation of or to harass any person for political, personal, or financial interest or gains without making an effort to get other person's point of view or not giving it proper coverage and space but does not include misinformation*"), and "misinformation" ("misinformation means verifiable false content or information that is unintentionally disseminated or shared"). Additionally, the bill imposes higher financial penalties for those intentionally spreading false news.

In **Cyprus**, a 'fake news' bill has been under discussion for several months. This proposed legislation aims to criminalize personal insults online, responding to growing concerns in the country. The main objective of the proposal is to safeguard the public from online attacks.

c) Illegal and Harmful Content

Illegal and harmful content poses threats to physical safety, online security, mental health, and overall well-being of individuals. It can inflict severe and lasting harm on victims and society as a whole [6]. Illegal content spans multiple jurisdictions, encompassing terrorist, violent, and extremist content, gender-based violence, and child sexual exploitation including Child Sexual Exploitation and Abuse (CSEA) material. Additionally, damage occurs with content that, while not necessarily illegal, still inflicts harm on others, such as material promoting eating disorders and self-harm, online public shaming, harassment, and trolling, etc.

Numerous online platforms voluntarily adopt content moderation techniques and establish policies and procedures to tackle specific illegal content, such as child CSEA or terrorist violence and extremism content (TVEC). To tackle this, the OECD[6] has introduced the Voluntary Transparency Reporting Framework[18]. This framework serves as an international and standardized hub for transparency reporting, allowing any online platform, regardless of its size or business model, to report on their content moderation methods and other strategies related to TVEC on their platform.

Some examples of how the challenge of Illegal and harmful content is being tackled globally are included below.

i. Globally

To address the unwanted side effects of emerging technologies, the European Union has introduced new rules to regulate Video-sharing platforms (VSPs) [63]. The regulations seek to ensure that VSPs implement suitable and efficient measures to safeguard individuals from specific types of illegal and harmful content present on their platforms.

One of the most significant changes came with a directive in 2018. This directive, known as the new Audiovisual Media Services Directive (AVMSD)[63], aimed to actively involve VSPs in the control and moderation of their content. The **European Commission** has requested the European Audiovisual Observatory to prepare a mapping report on how the rules applicable to VSPs have been transposed into national legal frameworks.

In **France** (mandates for online companies involve the removal of specific content deemed "manifestly illicit" within a 24-hour timeframe upon receiving notification)[64] and **Germany** (obliges social media platforms to eliminate hate speech and any other content deemed illegal)[65], there are rules regarding illegal and harmful content that cover specific types of illegal content as defined under the criminal code (and the legislation on the freedom of the press in France).

Cyberbullying has indeed been one of the primary domains of illegal and harmful content that has witnessed significant developments globally.

Italy [66] has targeted initiatives to combat specific types of illegal content, such as cyberbullying. Italy has been a pioneer in the introduction of cyberbullying in its judicial system with law 71/2017.

In the **United States**, nearly all states (for example, California [67] and Missouri [68]) have revised and enacted state laws and legislation to tackle cyberbullying and harassment through electronic communications. Some of these laws require evidence of 'ongoing harassment,' while others have been specifically introduced to combat cyberbullying and online abuse.

Ireland [69] has enacted new laws to address cybercrime. Cyberbullying is punishable under these laws, which include intentional victim shaming, encompassing the sharing or distribution of sexually explicit or intimate images of another person without their consent.

China [70] recently issued guidelines to impose strict penalties for cyberspace violations targeting minors, involving paid posters, fabricating 'sexual' topics, and utilizing artificial intelligence to disseminate illegal information.

ii. Examples from the DCO Member States

Children are particularly vulnerable targets when it comes to potentially harmful content. The cases of child sexual abuse material exposed online have increased by 87% since 2019 (2019-2022), with an additional 32 million reports worldwide, according to data from the Global Threat Assessment [71].

Ghana has had a law in place since 2020 that ensures the protection of children in the online context, known as the Cyber Security Act 10 (38) [72]. This law criminalizes child online abuses, including the production, viewing, and distribution of child sexual abuse materials, online grooming of children, cyberstalking of a child, and sextortion.

However, risks also extend to illegal content when it infringes on copyright laws. **Bahrain** is one of the countries that already has laws penalizing copyright infringements. An example of this is the Legislative Decree No. (22) of 2006 [26] regarding the protection of authors' rights and related rights law, including online protection.

d) Privacy

The right to privacy is protected by Article 17 of the International Covenant on Civil and Political Rights (ICCPR) [73], 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).

The OECD's Privacy Guidelines [74] established the basic principles for privacy protection, with a view to promoting trust and facilitating cross-border flows of personal data.

However, new technologies have significantly impacted how personal information is collected and used, posing increasing challenges to online privacy and personal data protection. Issues such as consent, substantive and temporal limits on the storage or use of collected information, and even the definition of personal information itself, are highly relevant. The protection of brain data, as offered by the Chilean Constitution [75], highlights the timeliness of this topic. With the advent of more intrusive emerging technologies, alarm around the need to address the challenge of privacy in the online world is growing stronger.

Some examples of how the privacy challenge is being addressed globally are included below.

i. Globally

As social and economic activities continue to migrate online, the significance of privacy and data protection is gaining heightened recognition.

Equally concerning is the collection, use, and sharing of personal information with third parties without the notice or consent of consumers. Among 194 countries globally, 137 have enacted legislation to ensure the protection of data and privacy [76].

Despite various proposals put forth over the years, there is still no comprehensive federal law governing data privacy in the **United States**. The American Data Privacy Protection Act (ADPPA) [77] has progressed further in the legislative process than its predecessors, but it continues to face significant obstacles. However, the United States does have numerous sectoral data privacy and data security laws at State level.

As previously mentioned, the **European Union** is the primary legal authority concerning data protection, emphasizing the importance of privacy. Across the EU members, the EU General Data Protection Regulation (GDPR) [22] regulates the processing and transfer of personal data of individuals. The GDPR stands as a comprehensive privacy law applicable to businesses of all sizes and sectors, replacing the Data Protection Directive 1995/46. The fundamental goals of these regulations remain consistent: setting out guidelines for safeguarding personal data and facilitating the use of personal data.

ii. Examples from the DCO Member States

Qatar took a pioneering step in the **GCC region** by enacting a comprehensive data protection law in 2016. The Data Protection Office [78], operating as an independent institution within the Qatar Financial Center (QFC), oversees the QFC Data Protection Regulations, which became effective on June 19, 2022. Both legislations impose substantial fines and restrictions, with ongoing efforts to enhance enforcement mechanisms.

In 2019, the government of **The Gambia** embraced the Data Protection and Privacy Policy (the Policy) [79], developed in consultation with the Council of Europe, establishing the groundwork for an institutional and legal framework for data protection and privacy.

Case Study

In 2022, the **Jordanian** government introduced new legislation named the Personal Data Protection Law (PDPL) [80] to Parliament. The law was approved and came into force in 2024. This law is designed to safeguard individuals' privacy by overseeing the collection, use, storage, and disclosure of personal data. The PDPL is applicable to both public and private entities processing personal data in **Jordan**. The law defines personal data as any information that can directly or indirectly identify an individual, such as names, addresses, phone numbers, email addresses, and social security numbers, among others. According to the law, personal data can only be collected for specific purposes and with the consent of the individual. Under the PDPL, entities are mandated to implement suitable measures to safeguard personal data from unauthorized access or disclosure. This includes adopting technical and organizational measures to ensure the security of personal data. An important aspect of the PDPL is that it grants individuals specific rights over their personal data. These rights include the ability to access their personal data held by an entity, correct any inaccuracies, and request the deletion of their personal data under certain circumstances.

The **Oman** Personal Data Protection Law (PDPL) [81] was officially issued on 9 February 2022 and became effective as of 13 February 2023. This law supersedes Chapter 7 of the Electronic Transactions Law and introduces significantly enhanced privacy provisions and fundamental data protection principles. The aim is to harmonize Oman's data protection framework with international standards.

Saudi Arabia recently enacted the Personal Data Protection Law [82] with notable extraterritorial implications. This law extends its jurisdiction to all personal data processing within the Kingdom and to processing activities conducted outside the Kingdom concerning data subjects within Saudi Arabia. Non-compliance can result in substantial fines, reaching up to $1.3 million. One significant change introduced by this law is the elimination of the requirement for exceptional approval from the Saudi Authority for Data and Artificial Intelligence (SDAIA) for international transfers. Although registration is not mandatory, the SDAIA will establish the criteria for data protection activities, license auditors and accreditation entities, and maintain a national register.

e) Security and Safety

Today, ensuring safety and security online has become a critical consideration underlying the use of new technologies. The threats are myriad and continue to grow as these technologies become increasingly vital in both people's lives and the global economy. Safeguarding security and online safety involve tackling a diverse array of challenges such as cyber threats, data breaches, identity theft, phishing attacks, online harassment, and the dissemination of misinformation. Effectively addressing these issues necessitates implementing strong cybersecurity measures, raising user awareness, developing effective policies, and fostering international cooperation. These efforts are essential to creating a secure digital environment for individuals, businesses, and organizations alike.

The global indicator for the 'Estimated Cost of Cybercrime' in the cybersecurity market is projected to experience a continuous rise from 2023 to 2028, reaching a total of 5.7 trillion U.S. dollars (+69.94 percent). Following eleven consecutive years of increase, the indicator is expected to reach a new peak of 13.82 trillion U.S. dollars in 2028[83]. In the first half of 2022, there were approximately 236.1 million reported ransomware attacks globally[84].

Rights such as the right to security and digital safety emerge as a response to the significant challenges posed in the online space. The right to online safety signifies the fundamental entitlement of individuals to utilize the internet and digital technologies securely. It involves protection against a spectrum of online threats, spanning from cyberbullying and identity theft to online harassment and data breaches. This fundamental right assures individuals the freedom to navigate the online realm without apprehension, confident that their personal information and privacy are shielded.

Just as this right applies to people, it should also be extended to businesses and organizations that have a substantial online presence today. The digital economy will be strengthened by the success in addressing this challenge.

Some examples of how the security and safety challenge is being addressed globally are included below.

i. Globally – Portugal Example

Case Study

ESET, a leading global cybersecurity firm, recently published the European Cybersecurity Index [85], a comprehensive study unveiling the varying levels of online safety across the European countries. The study assessed seven key cybersecurity factors, assigning a score out of ten for 24 European nations. The results indicate that **Portugal** boasts the highest level of cybersecurity, whereas Romania ranks the lowest. Factors considered included the number of cybersecurity laws in place, the percentage of residents in each country affected by banking or card fraud in the last three years, and the percentage of individuals in each nation whose social network or email accounts were hacked within the same period.

Considering this study, Portugal stands out notably due to its national strategy and legal adjustments aligned with the guidelines of this strategy. The Portuguese government unveiled its National Strategy for Cyberspace Security [86] for the period 2019 – 2023 in June 2019. This strategy emphasizes combating cybercrime and enhancing cybersecurity and cyberdefense. Cybercrime is defined as offenses outlined in the Cybercrime Law and other criminal activities carried out using technological means, where these means are essential for the execution of the crime. The strategy is structured around three core objectives: (I) enhance resilience; (ii) foster innovation; and (iii) generate and ensure resources.

Furthermore, institutions dedicated to these objectives have been established. Enshrined in Law no. 46/2018 [87], dated August 13, these institutions ensure the mobilization of resources, knowledge, and expertise necessary to address the intricate challenges and extensive scope of cybersecurity. Notably, these include:

- The High Council for Cyberspace Security: this specific consultative body operates in collaboration with the Prime Minister and comprises representatives from various stakeholders. It facilitates political-strategic coordination for cyberspace security.
- The National Cybersecurity Center: serving as the National Cybersecurity Authority and the primary national point of contact for international cybersecurity collaboration, this center plays a pivotal role in ensuring comprehensive cybersecurity efforts.

ii. Examples from DCO Member States

Like other countries, many DCO Member States are also experiencing escalating losses from cyberattacks each year. In 2020, according to IBM data [88], the average cost of a cyberattack on an organization in **Saudi Arabia** and the United Arab Emirates was $6.53 million, marking a 69% increase compared to the global average.

Saudi Arabia has implemented two distinct laws to address cybersecurity challenges in the digital world. Firstly, the Anti-Cyber Crime Law [89] comprises sixteen provisions defining key terms, scope, objectives, penalties, and fines related to cybercrimes. This law is designed to facilitate secure data exchange, protect the rights of computer and internet users, preserve public interest, morals, and individual privacy. Secondly, the Electronic Transactions Law [90] has been established to control, regulate, and establish a legal framework for electronic transactions.

In 2018, **Rwanda** enacted a cybercrime law [91] designed to aid both the government and the private sector in combating online crime. The proposed legislation aims to protect private and government information and infrastructure from online crimes and cyber-attacks. It empowers the government's security agencies to investigate threats, prosecute cybercrimes in private and public institutions, and defend the nation against cyber-attacks. Additionally, Rwanda recently inaugurated a regional cybercrime investigation center [92] that will coordinate efforts in Eastern Africa to investigate cybercrimes and cyber-enabled offenses, including terrorism, trafficking, and money laundering.

In the same vein and as mentioned earlier, the new Cyber Security Act recently approved by the Parliament of **Bangladesh** aims to protect individuals from cyber-attacks.

To conclude, the digital rights landscape is intricately woven with challenges that demand collective global attention and proactive measures. The identified issues of digital divide, misinformation and disinformation, illegal and harmful content, safety and security, and privacy are not isolated concerns but interconnected threads shaping the experience of individuals in the digital economy. It is encouraging to observe a global response to these challenges through a myriad of regional and local initiatives, laws, and regulations. Whether through infrastructure investments, and digital literacy programs to bridge the digital divide, regulatory frameworks combatting misinformation, or cybersecurity measures enhancing safety and privacy, nations worldwide, and the DCO Member States are actively engaging with these issues. Going forward, it is crucial to foster continued collaboration, innovation, and vigilance to ensure that digital rights are not just protected but continually strengthened in the face of emerging complexities.

5

A SHORTLIST OF **DIGITAL RIGHTS**

A SHORTLIST OF DIGITAL RIGHTS

Several digital rights have been established and pursued globally to address the challenges outlined in the preceding section. As we mentioned earlier, each digital right aims to tackle more than one challenge. Amongst the numerous digital rights recognized worldwide, considering the reality and diversity of DCO Member States, the following digital rights have been selected, that stand out as the most relevant in the current context, in line with the global trends, and based on their relevance to the DCO Member States.

1. Right to protection against online misinformation
2. Right to digital literacy
3. Intellectual Property (IP) Protection Online
4. Online Privacy Protection
5. Right to digital security and safety
6. Right to personal digital identity
7. Safe Digital Space – Especially for children
8. Protection Against Algorithmic Bias

Tabe 2: DCO Strategic Roadmap for 2030

Digital Right	Brief description and its relevance to the challenge(s)	Relevance to the DCO 2030 Roadmap
Right to protection against online misinformation	This digital right seeks to address the challenge of misinformation and disinformation, as well as the challenge of the digital divide, as the asymmetry in the use of new technologies can exacerbate the proliferation of misinformation and disinformation.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 2 – Data-driven Digital Economy, Objective 2.1. – encourage evidence-based and data-driven decision-making for all businesses and governments by facilitating access to the DCO's data and insights.
Right to digital literacy	This digital right focuses primarily on addressing the challenge of the digital divide, which is mitigated when there is a reinforcement of digital literacy.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 3 – Responsible Digital Economy, Objective 3.2. – Empower people by improving the quality, access, inclusiveness and interoperability of digital public goods and services among DCO Member States.
Intellectual Property (IP) Protection Online	This digital right aims primarily to address the challenge of illegal and harmful content, as the protection of intellectual property seeks to safeguard against the violation of protected content.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 1 – Thriving cross-border digital market, Objective 1.3. – Foster a business-friendly environment to attract digital investment and spur business creation across the DCO ecosystem.

Online Privacy Protection	This digital right aims to address the challenge of privacy, which could be strongly threatened, especially with the advent of emerging technologies like AI.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 2 – Data-driven digital economy, Objective 2.2. – Maximize the value of cross-border data flows by harmonizing data governance, policies, and regulations.
Right to digital security and safety	This right aims to address the risks posed by the challenge of safety and security, where the security of user data and transactions is, for example, strongly threatened.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 3 – Responsible Digital Economy, Objective 3.1. – Promote a safe digital space for children and the most vulnerable segments of society across the DCO ecosystem.
Right to personal digital identity	This right aims to address the challenge of the digital divide, safety and security, as well as privacy, insofar as access to a digital identity facilitates participation in the digital economy, and the protection of personal digital identity ensures the security and privacy of individuals in the context of using new technologies.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 3 – Responsible Digital Economy, Objective 3.2. – Empower people by improving the quality, access, inclusiveness and interoperability of digital public goods and services among DCO Member States.
Safe Digital Space – Especially for children	Aims to address the challenge of safety and security for children, as well as their privacy and protection against illegal and harmful content. It is a robust right that tackles various challenges.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 3 – Responsible Digital Economy, Objective 3.1. – Promote a safe digital space for children and the most vulnerable segments of society across the DCO ecosystem.
Protection Against Algorithmic Bias	This right aims to address the challenge of the digital divide, which is reinforced by algorithmic bias, especially in the wake of recent AI advancements. It also addresses safety and security concerns.	In the framework of DCO's Strategic Roadmap 2030 it is relevant to: Goal 3 – Responsible Digital Economy, Objective 3.2. – Empower people by improving the quality, access, inclusiveness and interoperability of digital public goods and services among DCO Member States.

The following parts of this section examine what each of the above-mentioned digital rights entail and what challenges they aim to address, with an ultimate ambition to create a digital environment that is inclusive, secure, and fair for everyone.

a) Right to protection against online misinformation

As discussed earlier, today's digital environment provides fertile ground for the rapid dissemination and amplification of false narratives, leading to widespread consequences.

The Right to Protection Against Online Misinformation refers to the right to safeguard citizens or society from false information disseminated with malicious or bad faith intentions, causing harm. This right has the following three key elements:

1. Access to Accurate Information: Individuals should have access to accurate and reliable information online. This includes access to fact-checked news sources, transparent reporting, and credible information sources.

2. Media Literacy and Education: People should be equipped with the necessary skills and knowledge to critically evaluate information they encounter online. Media literacy education helps individuals identify misinformation and disinformation, understand biases, and navigate the complexities of the digital information landscape.

3. Regulation and Accountability: There should be mechanisms in place to regulate online content and hold platforms, publishers, and users accountable for spreading false or misleading information. This may involve legal frameworks, policies, and enforcement mechanisms to address the dissemination of misinformation and disinformation online.

In recent years, the proliferation of disinformation and misinformation has reached alarming levels, particularly in the online sphere. Research[93] indicates that disinformation has become an intrinsic part of our information landscape, necessitating a nuanced approach in our efforts to combat it.

Disinformation erodes trust in essential institutions and scientific knowledge. It undermines core values such as diversity, tolerance, and openness, endangering both individual and public health, especially during the crisis times.

One challenge posed by misinformation/disinformation is that it often doesn't fit into any category of illegal content. This was particularly evident during the COVID-19 pandemic, where online content, while not breaking any laws, posed a threat to public safety. Governments faced a significant challenge in managing the sheer volume of information that diverged from factual accuracy and contradicted scientific evidence during this time.

Another challenge stemming from the widespread dissemination of misinformation is the insufficient media literacy skills among online users, hindering their ability to accurately discern the credibility of the information they consume.

Protecting people's right to be shielded from misinformation and disinformation is crucial. Equally important is equipping individuals with the necessary skills and tools to verify the credibility of the information they encounter. This empowers individuals to make informed decisions, promotes critical thinking, and strengthens resilience against the harmful effects of false information in the digital age.

b) Right to digital literacy

Digital literacy refers to the ability to access, understand, and effectively use digital information and technologies. Indeed, unequal access to digital skills compromises the global development of the Digital Economy and leads to social exclusion. Addressing this inequality should be a priority for governments and policymakers.

It is crucial to contextualize the concept of digital literacy historically [94]. 3000 years ago, literacy meant being an effective public speaker, mastering the art of persuasion through language. With Gutenberg, the inventor who originated a method of printing from movable type, literacy expanded to encompass reading and writing skills. The advent of portable cameras facilitated the production and distribution of images, leading to the introduction of visual literacy, emphasizing the ability to interpret images and understand their communicative power. The rise of databases ushered in powerful technologies, demanding new skills for searching, evaluating, and using information, giving birth to information literacy. The proliferation of TV channels prompted the need for media literacy, teaching individuals to navigate diverse media sources effectively. The introduction of microprocessors into our daily lives led to the emergence of an ICT-literate generation, requiring a whole new set of technical skills to harness the full potential of technology.

Since Paul Gilster's seminal work on Definitions of Digital Literacy [95], there has been a growing consensus on the term digital literacy, acknowledging the evolving skills needed to thrive in our digitally interconnected world.

It is contended that digital literacy serves as a foundational element for the full realization of individuals' fundamental right to the internet, as established in some countries.

When addressing the right to digital literacy, it's essential to delve into its multidimensional aspects.

1. Firstly, there's the capability to use digital tools effectively. This involves basic skills such as navigating the internet, using software applications, and operating digital devices competently.
2. Secondly, understanding the digital realm encompasses knowledge about online safety, data privacy, cybersecurity, and critical evaluation of digital content. It also includes comprehension of digital rights and responsibilities in the digital ecosystem.
3. Lastly, the dimension of creating within the digital realm involves the capacity to generate digital content, collaborate online, and participate in digital communities. This aspect emphasizes creativity, innovation, and the ability to contribute meaningfully to digital platforms and spaces.

Together, these three dimensions of digital literacy empower individuals to engage confidently and responsibly in the digital world, promoting digital inclusion and participation.

c) Intellectual Property (IP) Protection Online

The protection of Intellectual Property (IP) is crucial in the digital world and the online sphere. It is within this framework that the right to intellectual property online protection emerges.

Safeguarding IP in the digital space is essential to foster innovation, drive economic expansion, generate employment opportunities, and uphold the rights of both creators and consumers. It serves as a cornerstone in molding the digital economy and ensuring a level playing field for fair competition.

Generally, Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs, and symbols, names, and images used in commerce, according to the World Intellectual Property Organization (WIPO) [96].

IP is safeguarded by various laws which have created a patchwork of individual rights that protect different aspects of intellectual creations, like patents, copyrights, and trademarks, allowing individuals to earn recognition or financial benefits from their innovations or creations. The IP system aims to strike a balance between innovators' interests and the broader public interest, creating an environment where creativity and innovation can thrive, whilst sufficiently protecting and rewarding creativity.

With the emergence of Generative AI and other emerging technologies, IP has gained a refreshed global importance because of its profound influence across different facets of society, the economy, and daily existence, emerging technologies are exerting a transformative effect.

Tools like Digital Rights Management (DRM) technologies and strategies can be used to protect digital content from unauthorized access, copying, and distribution. DRM systems are designed to enforce copyright and licensing terms for digital assets.

d) Online Privacy protection

Privacy is acknowledged as a key digital right by nearly every nation across the globe through various means such as constitutional provisions or other legal frameworks.

The right to privacy, or the freedom to lead a private life, is firmly embedded in the Universal Declaration of Human Rights [1], specifically in Article 12.

However, the right to privacy often intersects with competing public interests, such as national security. Balancing these concerns becomes a complex task in legal and ethical frameworks.

The right to online privacy protection encompasses control, security, and transparency in the use of users' personal information on the internet.

The intricate matter of online privacy revolves around how an individual's personal information is gathered, processed, utilized, shared, and stored on their personal devices and while navigating the Internet.

Online privacy encompasses the security measures available for personal and financial data, communications, and preferences in the online sphere. Users commonly enhance online privacy by utilizing anti-virus software, selecting robust passwords, disabling tracking mechanisms, scrutinizing site security, and opting for stringent privacy configurations. Threats to online privacy span from phishing scams to malware, and vulnerabilities in website security can lead to identity theft.

Privacy protection in the digital space extends beyond individual rights; it forms the bedrock of trust, cybersecurity, and conscientious data stewardship today.

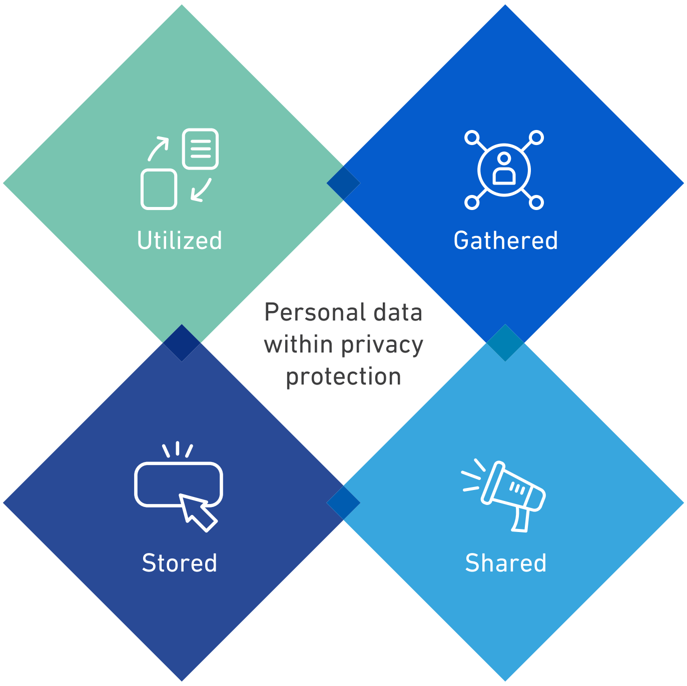


Figure 5: characteristics of the right to online privacy protection

e) Right to digital security and safety

Digital security and safety form integral aspects of broader digital rights, ensuring that individuals can actively participate in the digital world with confidence and trust in the security of their online interactions.

The right to digital security and safety denotes the inherent entitlement of individuals to protect their overall well-being while engaging in digital activities, using online services, and interacting with digital technologies. This encompasses the right to shield oneself from various digital threats, such as cyberattacks, online harassment, data breaches, identity theft, and other malicious activities that could compromise one's online presence and digital identity.

This right signifies that individuals should have the freedom to utilize digital technologies without the fear of unauthorized access or harm. Additionally, it imposes a responsibility on governments, organizations, and digital platforms to establish a secure online environment, implement robust cybersecurity measures, and uphold users' safety rights.

This right plays a pivotal role in shielding individuals, institutions, and even nations from a multitude of digital threats. It is indispensable for nurturing trust, upholding privacy, and preserving the reliability and cohesion of our globally interconnected digital landscape.
Digital security and safety can be safeguarded through a multifaceted approach that combines technological measures, awareness and education, policy and regulations, and collaboration among stakeholders.

f) Right to personal digital identity

Digital identity refers to the electronic representation of an individual, organization, or device when interacting in digital systems and transactions. In addition to helping establish and verify the identity of individuals and entities in the digital space, it is an important tool to improve access to reliable digital identity for displaced and stateless persons.

The right to own your digital identity is a fundamental human entitlement as it grants individuals the power to maintain control over their personal information, ensuring privacy and security in the digital domain. Moreover, it fosters inclusivity and equality, enabling individuals to actively participate in the digital economy.

In our modern, highly interconnected world, where our daily lives are intertwined with the digital realm, access to a credible digital identity system, and possessing ownership and authority over our digital identity is indispensable. It empowers us to navigate online platforms, conduct digital and financial transactions, and engage with others, all while preserving our autonomy and safeguarding our sensitive data.

A notable instance of acknowledging personal identity is witnessed in the European Union. Through the European Digital Identity [97], EU citizens, residents, and businesses have the means to confirm their identity or provide specific personal information. This digital identity solution serves a dual purpose, applicable for various public and private services both online and offline across the EU.

Some of the benefits of the European Digital Identity include:

EUROPEAN
DIGITAL IDENTITY

The entitlement of every eligible individual possessing a national ID card to possess a digital identity acknowledged across all EU member states

A convenient and secure method to manage the extent of information shared with services that necessitate personal data disclosure

Utilized through digital wallets accessible on mobile apps and other devices to:

1) Verify identities both online and offline

2) Store and exchange government-provided information such as name, surname, date of birth, and nationality

3) Share data from trusted private sources

4) Serve as proof of residency, employment, or educational status in specific EU member states

Figure 6: Benefits of the European Digital Identity

g) Safe Digital Space – Especially for children

Safe Digital Space for children means protection of children's rights in the digital space ensuring that children are shielded from potential harm, exploitation, and privacy breaches when using digital technologies, the internet, and social media platforms.

It recognizes the unique vulnerabilities of children in online settings and underscores the importance of creating a safe and secure digital environment for their well-being. This right is essential for fostering a positive and protective online experience for young users, considering that concerns vary depending on the ages of the children.

Ensuring the protection of children's rights in the digital space stands as a matter of utmost significance, as the digital environment profoundly shapes the lives of young individuals.

This commitment to safeguarding children's digital rights is indispensable to fostering their well-being, safety, and wholesome growth. It calls for collective responsibility, requiring the active involvement of parents, educators, policymakers, and society to cultivate a secure and nurturing digital landscape where children can flourish. Considering these aspects is vital to ensuring a safe, positive, and empowering digital environment for children.

When addressing the protection of children's rights in the digital space, several key aspects, needs consideration:

Online Safety: Ensuring children are protected from online threats, cyberbullying, and harmful content.

Privacy: Safeguarding children's personal information and online activities from unauthorized access or misuse.

Education and Awareness: Providing children with knowledge and awareness about online risks and safe digital practices.

Role of Guardians and Authorities: The responsibility of parents, guardians, teachers, authorities, and governments in protecting children online.

Impact of Social Media and Emerging Technologies: Understanding how social media platforms and new technologies affect children's digital experience and well-being.

Figure 7: Key aspects of the Right to Protection of Children's Rights in the digital space

h) Protection Against Algorithmic Bias

The Right to Protection Against Algorithmic Bias underscores individuals' fundamental entitlement to be shielded from discriminatory practices and biases propagated by algorithms, especially used in the Artificial Intelligence (AI) systems. As algorithms become ubiquitous in decision-making processes, including employment, financial assessments, legal proceedings, and content suggestions, ensuring fairness and equity is paramount.

This right highlights the necessity for transparency, fairness, and accountability throughout the entire lifecycle of an algorithm. It serves as a safeguard against unfair treatment, discrimination, and biases stemming from algorithmic decision-making. Upholding this right requires vigilance in addressing inherent biases, promoting diversity in data representation, and implementing measures to rectify and prevent discriminatory outcomes. Ultimately, it advocates for an ethical and just use of algorithms, fostering a digital landscape free from unfair prejudices.

The significance of safeguarding against Algorithmic Bias should not be underestimated, given the growing impact of algorithms across multiple facets of our daily existence. Individuals have the right to be protected from discriminatory or unfair outcomes resulting from algorithms in decision-making processes. As mentioned in DCO's Strategic Roadmap 2030, Algorithmic Bias potentially gives scientific credibility to human biases.

The European Union recently introduced the "Ethics Guidelines for Trustworthy AI" [98] to address and combat algorithmic bias. These guidelines outline seven essential governance principles:

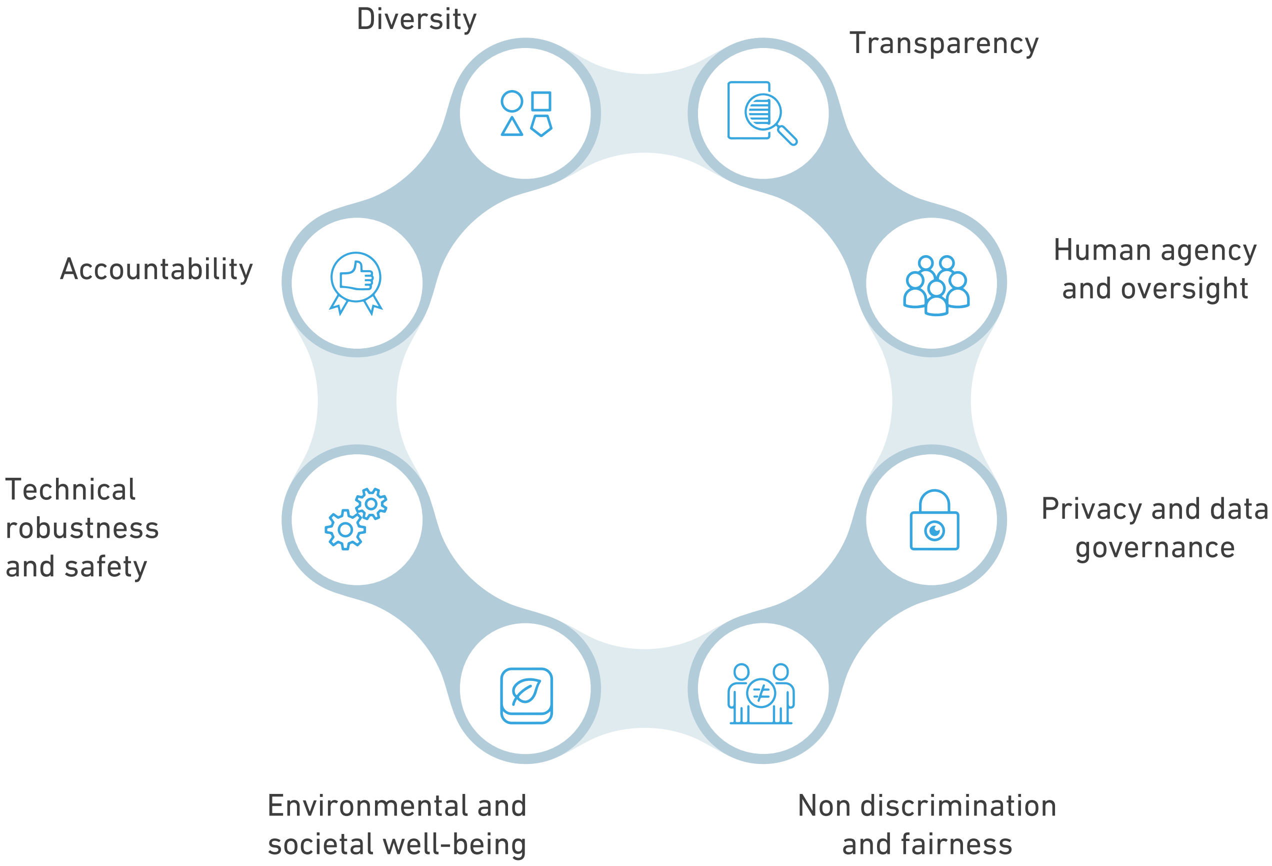
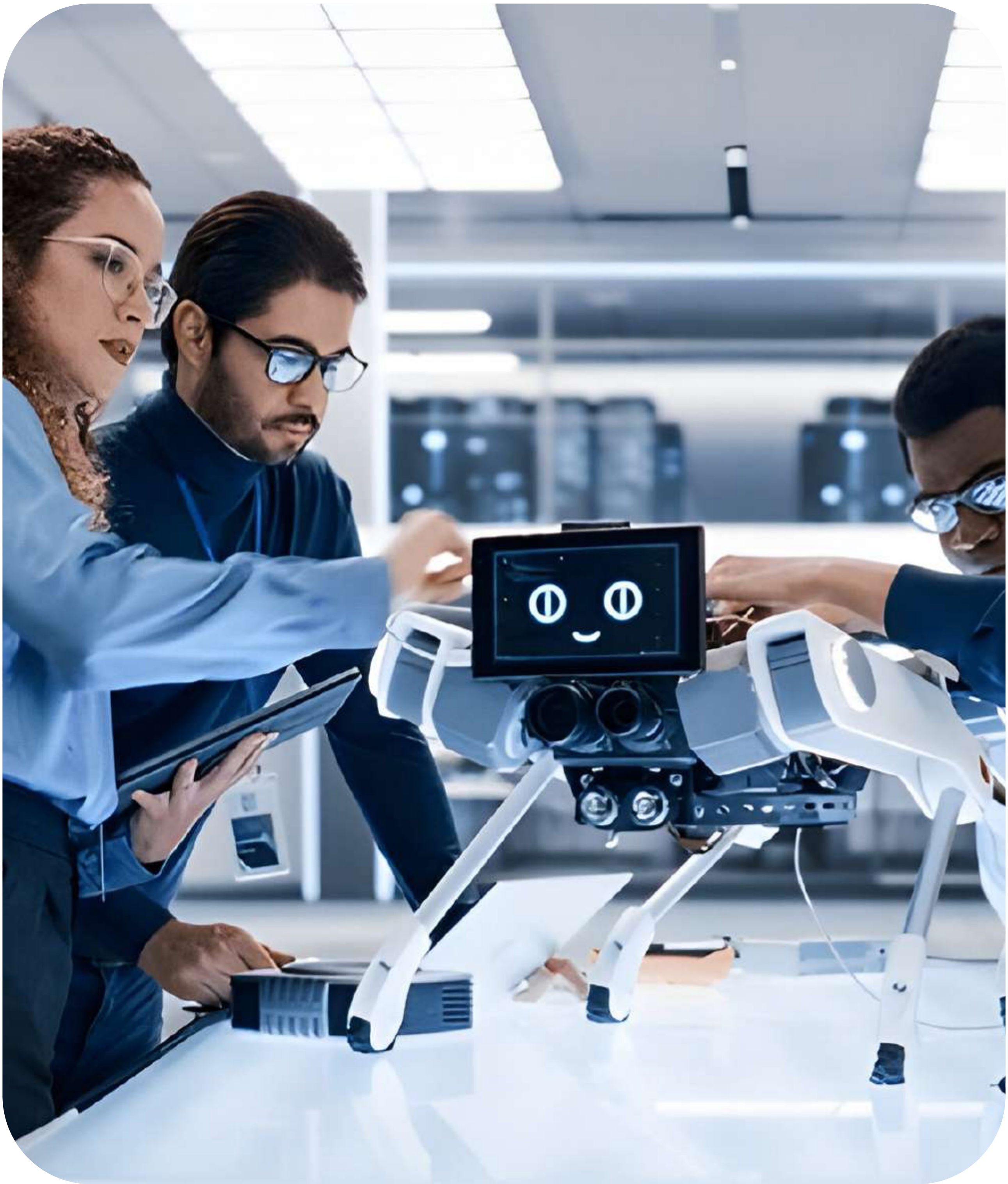

Diversity
Transparency
Accountability
Human agency and oversight
Technical robustness and safety
Privacy and data governance
Environmental and societal well-being
Non discrimination and fairness

Figure 8: Governance principles of the EU Ethics Guidelines for Trustworthy AI

This ethical framework represents a consensus that unfair discrimination is fundamentally unethical. Within these guidelines, member states emphasize the importance of linking diversity and non-discrimination to the principles of fairness. This approach fosters an inclusive AI ecosystem, ensuring equal access, inclusive design practices, and equitable treatment for all individuals throughout the entire lifecycle of AI systems. The EU's commitment to these principles reflects a significant step towards building ethical and unbiased artificial intelligence technologies.

The OECD has also provided recommendations[99] regarding the ethical aspects of Artificial Intelligence, addressing concerns related to algorithmic bias.



6 POLICY RECOMMENDATIONS ON THE SHORTLISTED **DIGITAL RIGHTS**

POLICY RECOMMENDATIONS ON THE SHORTLISTED DIGITAL RIGHTS

As we navigate the intricate landscape of digital rights, this final section serves as a compass, charting a course towards effective policy recommendations for the eight shortlisted digital rights explored in the preceding sections. Building upon the insights gained from scrutinizing the challenges and global initiatives surrounding these rights, our focus now shifts to formulating actionable recommendations. In a rapidly evolving digital realm, the intersection of technology, ethics, and governance becomes paramount. By proposing thoughtful policies measures, we endeavor to foster an environment where individuals can exercise their digital rights with confidence, where innovation coexists with responsibility, and where the digital landscape aligns with principles of inclusivity, security, and fairness.

This section serves as a call to action, urging stakeholders at all levels to collaboratively shape policies that not only protect but also enhance the digital rights crucial for a thriving and equitable digital future.

Right to protection against online misinformation

These recommendations aim to address one of the main conclusions of DCO's global roundtable held in Cape Town in November 2023:

- The reliability of information is now one of the internet's greatest challenges. Holding accountable the entities that manage digital platforms and improving the legal framework are priorities that should be embraced by states.

In response to the question about which digital rights should receive greater attention in today's context, the right to protection against misinformation garnered the highest number of choices in the surveys distributed to the roundtable participants. The concern about the issue of disinformation/misinformation is significant hence the emphasis on the below outlined recommendations:

Combatting disinformation/misinformation requires a multifaceted approach that involves individuals, communities, organizations, and governments. Accordingly, the following is recommended:

- Policymakers and legislators should partner with relevant subject matter experts in academia, NGOs, and relevant digital private sector entities to co-create guidelines and frameworks to support **legislation on misinformation and disinformation** in the online sphere.
- **Media literacy programs** should be developed to educate people, especially students, on how to critically evaluate information sources, fact-check claims, and identify bias.
- **Fact-Checking Initiatives** are advised to support and promote the debunking of false information and provide accurate information to the public.
- Media outlets and organizations should establish **transparency measures** by disclosing funding sources, affiliations, and potential biases.
- Regulatory and legislative approaches should be developed to combat misinformation, such as **laws requiring transparency in online advertising** or holding platforms accountable for the spread of false information.
- Provisions should be developed to ensure **inclusivity and diversity** are taken into consideration **in the online advertising industry**.

Right to Digital Literacy

Regarding digital literacy, the recommendations outlined below are aligned to one of the most important conclusions from DCO's GCC roundtable held in Riyadh in September 2023:

- The widespread use of new technologies today underscores the need to invest in digital literacy. Whether for children or adults, digital literacy should be a focus for governments.

The consensus among participants was that promoting literacy and 'awareness' represents the most effective approach for safeguarding this digital right. Awareness emerged as the most commonly used term during the discussions, emphasizing the need to enhance peoples' knowledge and understanding on the risks and opportunities associated to the use of digital technologies.

The recommendations below are inspired by the most innovative initiatives taken to promote digital literacy by governments, civil society organizations, and other stakeholders globally.

- Governments dedicated to education and training should partner with schools, educational institutions, and teachers to establish national/regional digital literacy strategies with robust educational components to empower more citizens to engage meaningfully online, considering the following elements:

- Guaranteeing diverse representation from communities and stakeholders
- Facilitating fair access to community-driven programs
- Encouraging continuous learning throughout life
- Advocating for digital citizenship and work towards bridging the digital gap
- Focusing on safety and digital wellness as top priorities
- Enhancing inclusion, accessibility, and active engagement of marginalized communities
- Strengthening collaborations between various levels of governance (local, provincial, national, regional and international)
- Defining the roles and obligations of the technology industry clearly
- Incorporating continuous assessment and adaptation to ensure openness and accountability
- Securing sufficient and enduring funding

Government officials involved in education and training should partner with schools, educational institutions, and teachers, along with companies/organizations in the technology sector to **develop** and **promote digital literacy skills programs**. One highly successful program in this domain is the Canadian DigitalSmarts program [100], which includes a series of workshops designed to teach essential everyday digital skills especially for the under-represented populations. These workshops cover areas such as online privacy and security, job searching, online shopping and banking, effective social media use, internet searching techniques, and managing screen time for kids. This program offers digital resources, in addition to in-person workshops.

Online Privacy Protection

The below outlined recommendations are aligned with one of the main conclusions of the Global roundtable that took place in Geneva in December 2023:

- The ease with which privacy is exposed through internet usage today reinforces the need to hold public entities and technology organizations accountable. The development of national strategies is one of the options that states should pursue.

When asked about the digital rights that should receive greater attention, privacy garnered the highest number of choices in the distributed surveys at this roundtable. We have shaped our recommendations to address this concern.

In the field of **online privacy protection**, and considering **the OECD Privacy Framework** [101], the following has is recommended:

- Policymakers and legislators should partner with the industry, sectoral regulators and academia in the field of privacy protection to create **distinct regulatory bodies** (at national or regional levels) dedicated to enacting and enforcing data protection and privacy regulations, equipped with the necessary governance structure, resources, and technical proficiency to carry out their responsibilities effectively.
- Policymakers and legislators should partner with relevant academia and private sector to co-develop **national privacy strategies**, ensuring their alignment with existing and new strategies in related domains, such as online security (e.g., national cybersecurity strategies), considering factors, including but not limited to:
    - Legal framework
    - Data protection principles
    - Consent mechanisms
    - Data security measures
    - Data breach notifications
    - Cross-border data transfers
    - Regulatory oversight
    - International cooperation
- Higher education institutions should partner with other organizations related to education and training, along with experts in the field of privacy and privacy professionals to establish **credential programs in data protection and privacy**, along with **specialized education** and professional development services. Research has shown that the presence of **privacy professionals** in the digital national ecosystem plays an increasingly vital role in the execution and oversight of privacy management programs, outlining the necessary competencies for these professionals.
- International organizations, in collaboration with the private sector, innovators and academia should encourage the development, adoption and scaling of robust **Privacy Enhancing Technologies (PETs)** aimed at ensuring compliance with the established privacy standards.

Rights to Digital Security and Safety

Safety and security were highlighted as aspects of great relevance in the roundtables held in Riyadh, Cape Town, and Geneva:

- The risks facing internet users today are numerous, with one of the most significant being digital safety and security. Giving special attention to the most vulnerable, especially children, and developing national strategies for their protection should be a priority for states.

In the field of **digital security and safety**, and considering **the Global Principles on Digital Safety (World Economic Forum)** [102] the recommendations are as follows:

- Policymakers and legislators should partner with schools and educational institutions, citizens and the media to acknowledge the critical need to support vulnerable and marginalized communities in exercising their rights in the digital realm, **emphasizing the protection of children's safety and online privacy**.
- Policymakers and legislators should partner with tech companies and experts in the field of privacy protection to develop **national cybersecurity strategies**, ensuring their alignment with existing and new strategies in related domains, such as data protection, considering the following elements in these strategies:
  - Policy and governance
  - Legal and regulatory framework
  - National cyber incident response plan
  - Critical infrastructure protection
  - Public awareness and education
  - Cybersecurity standard and best practices
  - Continuous Monitoring and Risk Assessment
- International organizations, in collaboration with diverse public and private, national and trans-national stakeholders should develop **frameworks, tools, systems, and protocols on online safety and security** that are standardized across borders while respecting national sovereignty and local cultural/social values.

Rights to Personal Digital Identity

The right to personal identity was chosen as one of the major challenges in the Global roundtable held in Cape Town, as well as in the one in Geneva:

- The access to, and protection of personal digital identity should be on the agenda of all states. It is important, for this purpose, to hold private organizations such as digital platforms accountable, ensuring that they develop tools to safeguard personal digital identity.

The recommendations presented below align with this concern, seeking to address this challenge.

In the **field of personal digital identity, and considering the recommendations of OECD** [103], the following is recommended:

- Policymakers and legislators should partner with private companies such as digital platforms, and experts in the field of technology and systems development to **develop and deploy digital identity systems** tailored to the requirements of users and service providers, while considering the national context, including digital readiness and ongoing digital identity initiatives. This approach should be integral in the design, implementation, or enhancement of any digital identity system, ensuring alignment with domestic needs and existing progress in digital identity initiatives. To achieve these goals, the following aspects should be considered:

- Policymakers and legislators should partner with private companies such as digital platforms, and experts in the field of technology and systems **development to develop and deploy** digital identity systems tailored to the requirements of users and service providers, while considering the national context, including digital readiness and ongoing digital identity initiatives. This approach should be integral in the design, implementation, or enhancement of any digital identity system, ensuring alignment with domestic needs and existing progress in digital identity initiatives. To achieve these goals, the following aspects should be considered:

  - **Promote Access and Equity:** ensure accessibility, affordability, usability, and fairness throughout the digital identity lifecycle, making secure and trusted digital identity solutions accessible to all, especially vulnerable groups and minorities, catering to their specific needs.

  - **Preserve Access to Essential Services:** Guarantee that access to essential services, both public and private, is not limited or denied to individuals who choose not to or cannot use digital identity solutions.

  - **Raise Awareness and Ensure Security:** Educate the public about the benefits and secure usage of digital identity, highlighting how the system protects users. Acknowledge potential risks and demonstrate effective measures to mitigate harm.

  - **Provide Support and Skill-building:** Establish support channels to assist individuals facing challenges in accessing and using digital identity solutions. Identify opportunities to enhance users' skills and capabilities.

  - **Monitor, Evaluate, and Report:** Implement robust monitoring and evaluation mechanisms, publicly reporting on the effectiveness of the digital identity system. Focus on inclusivity and work towards minimizing barriers to access and usage of digital identity solutions.

- Policymakers and legislators should partner with tech companies and digital platforms to guarantee that policies and legal frameworks in the design, development, and implementation of digital identity systems ensure transparency, accountability, and alignment with user needs and expectations, shaped through **active engagement and participation of stakeholders, and according the Guidelines of the Council of Europe** [103]. It is important to provide opportunities for stakeholders to review policies and laws before their adoption. Additionally, publish the outcomes of stakeholder engagement efforts, promoting transparency and accountability in the decision-making process.

- International organizations should collaborate with the national governments to foster global/regional cooperation for establishing **interoperability among various national digital ID systems,** thereby facilitating a seamless cross-border digital economy. These initiatives can be advocated and implemented through means such as bilateral or multilateral digital trade agreements.

Protection Against Algorithmic Bias

The right to be protected from algorithmic bias was one of the most frequently chosen ones in the Global roundtable in Cape Town as deserving greater attention:

- The need to involve stakeholders in the solutions to protect citizens against algorithmic bias is crucial, working on robust regulatory frameworks that can be effective.

The recommendations presented below aim at achieving this goal.

Considering the numerous ethical issues associated with **algorithmic bias** and the resulting harm, the following is recommended:

- Policymakers and legislators should partner with international organizations, technology companies, and AI developers to develop **ethical AI governance standards**. These standards should aim to safeguard the key ethical concerns relevant to the design, development, deployment and use of AI.
- Policymakers and legislators should conduct a thorough **review and adaptation of policy and regulatory frameworks,** along with assessment mechanisms related to AI systems. This adaptation should encourage innovation and foster healthy competition in the realm of trustworthy AI, working closely with stakeholders to promote the responsible use of AI in workplaces, enhancing worker safety, job quality, entrepreneurship, and productivity. The aim should be to ensure that the benefits derived from AI are distributed widely and equitably.
- International organizations should establish and advocate for global standards and guidelines for algorithmic fairness and transparency. They should facilitate **cross-border collaboration** among governments, tech companies, and researchers to develop best practices for identifying and mitigating bias in algorithms used in various domains such as healthcare, finance, and criminal justice.
- International organizations, with support of international technology and policy experts should develop frameworks and tools to ensure that global development of algorithms and AI tools is ethical and responsible by design, taking into consideration all aspects related to the protection of human rights.
- Technology companies should prioritize diversity and inclusivity in their workforce, particularly in data science and algorithm development teams to minimize biases in their products. Technology companies should implement rigorous testing protocols to identify and rectify bias in algorithms before deployment, leveraging diverse datasets and comprehensive evaluation frameworks.

7

CONCLUSION

CONCLUSION

Digital rights have become an inescapable aspect of the modern world, particularly in the context of a rapidly expanding digital economy where technology permeates every facet of society. The prevalence of online interactions brings forth numerous challenges and risks, prompting countries to adopt diverse approaches while grappling with ever-evolving developments in this arena.

Throughout this policy paper, we have presented recommendations pertaining to digital rights, carefully tailored to the realities of DCO Member States, global trends, and the emergent issues therein. To this end, we have identified eight digital rights crucial for safeguarding, protecting, and enhancing digital freedoms, encompassing protection against online misinformation, digital literacy, intellectual property (IP) rights online, online privacy, digital security and safety, personal digital identity, safeguarding children's rights in the digital sphere, and protection against algorithmic bias.

Protection of these rights, as delineated in the paper, align with the objectives and flagship actions outlined in DCO's Strategic Roadmap 2030, aiming to tackle the challenges encapsulated within five primary categories: digital divide, misinformation and disinformation, illegal and harmful content, safety and security, and privacy concerns.

Within the framework of these eight rights, recommendations have been presented, highlighting the significance of engaging relevant stakeholders in the policy formulation process. It is imperative to underscore that these recommendations are informed by comprehensive primary and secondary research, including insights gleaned from roundtable discussions held over several months.

This paper aims to serve as a foundational step towards devising a comprehensive and nuanced approach to address the predominant challenges facing the digital economy concerning digital rights. It is a contribution intended to bolster the collective response to furthering the key digital rights, aligning with the imperative to foster the digital economy as a strategic driver for economic and social advancement within the DCO Member States.

ANNEXURE A

How are different countries defining and implementing digital rights?

Globally, there are several countries that have already addressed various digital rights through several legislative and policy initiatives.

Internet access has been established as a right in **Mexico** ever since the nation's constitution was amended in 2013 to ensure **universal online access** [104]. Mexico holds the distinction of being the first country in the world to constitutionally guarantee government-provided internet. The Mexican Government has launched a Digital Strategy program aimed at realizing the country's objectives in government transformation, digital economy, educational reform, universal and efficient healthcare, as well as civic innovation and citizen engagement. This initiative operates within a legal framework that encompasses open data, interoperability, and digital identity, emphasizing inclusion, digital skills, and connectivity.

The first country in the world to develop a **digital rights charter** was **Brazil** in 2014. The "Marco Civil da Internet" is a comprehensive law that essentially creates a **bill of rights for the internet** [105] in Brazil. The legislation was drafted through an open, collaborative process with contributions from various stakeholders, including private individuals and civil society organizations. Brazil's Internet Bill of Rights protects internet privacy and free expression, and new rights, like net neutrality. It codified ten principles developed by the country's Internet Steering Committee in the constitution, including network neutrality, freedom of expression and privacy, to define and grant strong civil rights for citizens both online and offline.

In Europe, **Italy** was the pioneering country to move forward with a digital rights charter. The "**Declaration of Internet Rights**" [106] was approved by the Chamber of Deputies in 2015. Italy's Declaration of Internet Rights protects rights such as privacy, identity, or self-determination within a digital context and introduces new ones, like the rights of people on platforms, and Internet governance. Italy also pioneered the '**Charter of Fundamental Rights of Digital Labor in the Urban Context**,'[10107] marking the first agreement of its kind. Signed in Bologna on May 31, 2018, following negotiations involving Riders Union Bologna, Italian Trade Unions CGIL, CISL, and UIL, the Municipality of Bologna, and various platforms, the Charter is structured into four chapters. These chapters encompass general provisions, the right to be informed, the right to protection (including fair wages, health and safety, protection of personal data, and the right to disconnect), and support from public administration. It's important to note that the charter is non-binding; only those who voluntarily sign it are obligated to adhere to its principles.

In 2021, **Colombia** declared **internet access to be an essential public service**. The service must be provided in an efficient, continuous and permanent manner, guaranteeing connectivity among all the inhabitants of the national territory, and especially for the population that due to its social or ethnic condition is in a vulnerable situation or in rural and remote areas. Colombia has recently initiated discussions on a proposed Bill[108] that seeks to address legal and ethical concerns surrounding the creation, distribution, commercialization, and utilization of AI.

Furthermore, in South America, in 2021, **Chile** became the first country to include "**brain rights" in its constitution** [109], with the aim of protecting mental privacy, free will, and ensuring non-discrimination in access to neurotechnology. The goal is to grant personal brain data the same legal status as an organ, preventing it from being bought, sold, trafficked, or manipulated. Earlier this year, the Chilean Supreme Court issued a landmark judgment regarding neurotechnology and human rights, addressing the increasingly significant issue of mental privacy. This case [110] is closely linked to the constitutional change, which incorporated the following into the constitution: *"Scientific and technological development will be at the service of people and will be carried out with respect for life and physical and mental integrity. The law will regulate the requirements, conditions and restrictions for its use in people, having to protect especially the brain activity, as well as the information coming from it"*. The Supreme Court ruling pertains to a product named Insight, marketed as an external headset that monitors users' brainwaves. This device can be utilized to track cognitive performance indicators such as attentiveness levels and stress, or even control various devices. In response, the court has mandated Emotiv, the neurotechnology company behind the product (which originated in Australia in 2011), to remove the brain data of one of their citizens from their platforms and cloud services. Additionally, regulatory bodies have been instructed to conduct a more thorough investigation into Emotiv's neurotechnological device.

In 2021, the **Spanish** Government adopted a **Digital Rights Charter** [111] to articulate a reference framework to guarantee citizens' rights in the new digital age. This charter established the protection of rights such as the right to data protection, right to identity in the digital environment, right to digital security, or child protection in the digital environment. Without being regulatory in nature, the text contains a set of principles and rights to guide future regulatory projects and the development of public policies in order to guarantee the protection of individual and collective rights in new digital scenarios. The Charter also aims to strengthen citizens' rights, create certainty for society in the new digital age and increase people's confidence in the changes and disruptions brought about by new technologies. This Charter seeks to update existing rights recognized in texts such as the **Declaration of Human Rights** in the Spanish Constitution, and to adapt them to the new circumstances of the digital age.

Since 2021, **Portugal** has also a digital rights charter. The Portuguese Charter was approved in 2021. This **Charter of Human Rights in the Digital Era** [112] outlines the rights, freedoms, and guarantees for citizens online. It consists of 21 articles, including the establishment of a social internet tariff, concerning the right to access the digital environment, recognizing rights to privacy. In essence, the Charter outlines both entitlements and responsibilities within the digital space, spanning various domains ranging from the expression of personal rights in the online sphere — encompassing privacy rights, digital identity, and other individual entitlements — to the manifestation of constitutionally safeguarded rights, liberties, and assurances in the virtual space. These include freedom to access the Internet, the right to express oneself and create within digital contexts, and the right to congregate, exhibit, affiliate, and engage within the digital landscape. The document has legal force since it was approved by the Portuguese Parliament.

In 2021, **Japan** also experienced several developments in these domains with the Japanese parliament passing 3 laws to promote a "digital society": the Basic Act on Forming a Digital Society [113], the Act on Establishing the Digital Agency [114], and the Act on Adjusting Laws Related to Forming a Digital Society [115]. The term 'digital society' signifies a dynamic environment where diverse information and knowledge are acquired, shared, and transmitted globally through the Internet and advanced networks, while leveraging technology to effectively harness the wealth of data available in electronic formats. The Basic Act outlines the fundamental approach toward developing core principles and strategies for shaping a digital society, defining the roles of governments, authorities, and enterprises. Furthermore, Japan has focused on specific recommendations regarding specific technologies. In 2022, Japan published AI governance guidelines.

Starting in 2023, the **United States** aims to introduce **new data protection regulations** [115] in some states. In California, Colorado, Connecticut, Utah, and Virginia, the legislation will mirror the rights-based philosophical framework of GDPR. These new laws signify a holistic approach to privacy protection, encompassing various sectors and complementing existing sector-specific regulations. This development marks a significant stride in digital rights. It is noteworthy that the United States has had rules in place since 1998 to safeguard digital copyrights. The Digital Millennium Copyright Act (DMCA) was established to address the challenges posed by the digital age. Its primary objective is to modernize copyright laws for the digital landscape, safeguarding content creators' rights while encouraging innovation and creativity. Additionally, Congress is considering legislation to reform 'big tech.' In October 2023, President Biden issued a groundbreaking Executive Order [116] aimed at ensuring America's leadership in harnessing the potential and mitigating the risks of artificial intelligence (AI). This order sets forth innovative standards for the safety and security of AI. Through this Executive Order, the President sets forth a series of actions aimed at safeguarding against the potential risks posed by AI systems:

- Mandate that developers of the most powerful AI systems share their safety test results and crucial information with the U.S. government
- Develop standards, tools, and tests to ensure the safety, security, and reliability of AI systems
- Mitigate the risks associated with using AI to manipulate hazardous biological materials
- Safeguard Americans from AI-enabled fraud and deception by instituting standards and best practices for detecting AI-generated content and authenticating official content
- Establish an advanced cybersecurity program to create AI tools for identifying and addressing vulnerabilities in critical software
- Direct the formulation of a National Security Memorandum outlining further actions concerning AI and security

For several years, **Canada** has had the Personal Information Protection and Electronic Documents Act [117]. This law is designed to safeguard the privacy rights of internet users by mandating that organizations inform users about their data handling practices and obtain their consent to collect, use, and disclose personal information. The enforcement of this law has been instrumental in preserving digital rights, including the right to be forgotten. Recently, the Federal Court of Appeal rejected Google's attempt to challenge a decision that the company's search engine falls under Canada's privacy law. This ruling represents a significant victory for individuals advocating for a digital 'right to be forgotten.' The federal privacy commissioner had brought the case to the Federal Court, questioning whether Google's search engine should be exempt from the Personal Information Protection and Electronic Documents Act. The court's response has now arrived, dismissing Google's attempt to evade the regulations outlined in the act, thereby upholding the right to be forgotten.

Currently under discussion in **Australia** is the **Misinformation and Disinformation Bill** [118]. The primary objective of this draft Bill is to enhance transparency regarding the measures taken by digital platforms to manage seriously harmful misinformation and disinformation circulating on their services. It is also important to mention the **Online Safety Act 2021**[119]: it is recent legislation in Australia that significantly strengthens the country's existing online safety laws, making them more comprehensive and robust. This Act holds immense implications for online service providers, as it heightens their responsibility for ensuring the online safety of their users. Under this Act, the industry is mandated to formulate new codes aimed at regulating illegal and restricted content. These regulations encompass the most severely harmful materials, including videos depicting child sexual abuse or acts of terrorism, as well as content unsuitable for children, such as highly violent or explicit material.

In October 2023, the Cyberspace Administration of **China** has introduced its Global AI Governance Initiative [120], outlining a framework for artificial intelligence development. This framework advocates for equal rights in AI development, irrespective of a country's size, strength, or social system. It condemns the use of AI technologies for manipulating public opinion, spreading disinformation, interfering in other countries' internal affairs, social systems, and social order, as well as undermining the sovereignty of other states. The initiative calls for global collaboration to promote the responsible development of AI, sharing AI knowledge, and making AI technologies accessible to the public under open-source terms. It also emphasizes the need to establish a testing and assessment system based on AI risk levels, implement agile governance, and adopt tiered and category-based management for swift and effective responses. Research and development entities are urged to enhance the predictability of AI, improve data authenticity and accuracy, ensure continuous human control over AI systems, and create trustworthy AI technologies that can be reviewed, monitored, and traced. It advocates for a gradual establishment and improvement of relevant laws, regulations, and rules, with a focus on safeguarding personal privacy and data security in AI research, development, and applications.

REFERENCES

1 Universal Declaration of Human Rights, 1948

2 20th regular session of the Human Rights Council (18 June - 6 July 2012)

3 Guiding Principles on Business and Human Rights, United Nations, 2011

4 World Bank Report

5 Going Digital: making the transformation work for growth and well-being, OECD, 2017

6 Rights in the Digital Age: Challenges and Ways Forward, OECD, 2022

7 Human Rights and Digital Technology Resource Hub

8 Call to Action for Human Rights, United Nations, 2020

9 Roadmap for Digital Cooperation, United Nations, 2020

10 Digital Rights Governance Framework, UN Habitat

11 Our Common Agenda Policy Brief 5 A Global Digital Compact — an Open, Free and Secure Digital Future for All, United Nations, 2023

12 Recommendation of the Council on OECD Legal Instruments Broadband Connectivity, OECD, 2021

13 Recommendation of the Council on Artificial Intelligence, OECD, 2019

14 Recommendation of the Council on Children in the Digital Environment, OECD, 2022

15 Recommendation on Enhancing Access to and Sharing of Data, OECD, 2021

16 Recommendation on Digital Security of Critical Activities, OECD, 2019

17 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 2002
Recommendation of the Council on the Governance of Digital Identity, OECD, 2023

18 Voluntary Transparency Reporting Framework, OECD

19 European Declaration on Digital Rights and Principles for the digital decade

20 Charter of Fundamental Rights

21 2023 Report on the State of the Digital Decade

22 EU General Data Protection Regulation (GDPR)

23 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts

24 ASEAN Digital Economy Framework Agreement (DEFA)

25 Proposal of the Ibero-American Agreement of Digital Principles and Rights

26 Legislative Decree No. (22) of 2006, regarding the protection of authors' rights and related rights law, including online protection, Bahrain

REFERENCES

27 https://www.dataguidance.com/news/bangladesh-government-enacts-cybersecurity-act-2023

28 https://www.dataguidance.com/legal-research/gambia-information-and-communications

29 https://mofep.gov.gh/sites/default/files/acts/Ghana_DFS_Policy.pdf

30 https://www.dataguidance.com/opinion/greece-bill-emerging-technology-unified-framework

31 https://www.dataguidance.com/news/kuwait-citra-publishes-new-data-privacy-protection

32 http://www.cndp.ma/wp-content/uploads/2023/11/Loi-09-08-Fr.pdf

33 https://paradigmhq.org/report/digital-rights-and-freedom-bill-2019/#:~:text=This%20Bill%20seeks%20to%20protect,platforms%20and%2For%20Digital%20media

34 https://www.dataguidance.com/opinion/oman-new-personal-data-protection-law-%E2%80%93-what-you

35 https://www.pta.gov.pk/assets/media/digital_gender_inclusion_strategy_28-02-2024.pdf

36 Personal Data Protection, Qatar

37 https://dig.watch/resource/rwanda-child-online-protection-policy#:~:text=The%20Rwanda%20Child%20Online%20Protection,safely%20navigate%20the%20digital%20environment

38 https://www.my.gov.sa/wps/portal/snp/aboutksa/smartstrategy/?lang=en#:~:text=The%20Smart%20Government%20Strategy%20(2020%2D2024)%20defines%20the%20Kingdom's,and%20the%20Saudi%20Vision%202030

39 https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

40 Digital 2023 Global Overview Report

41 The United Nations Secretary-General's Roadmap for Digital Cooperation – Digital Human Rights, United Nations

42 Roundtables – Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation

43 https://www.fcc.gov/general/connect-america-fund-caf

44 https://usof.gov.in/en/bharatnet-project

45 https://www.digitale-doerfer.de/

46 https://www.gov.uk/government/publications/gigabit-broadband-voucher-scheme-information

REFERENCES

47 Bahrain eGovernment National Strategy

48 Electronic Participation Policy Kingdom of Bahrain, 2023

49 Vision Djibouti 2035, Republic of Djibouti

50 Djibouti Country Partnership Framework (CPF) 2022 - 2026

51 Infodemics and misinformation negatively affect people's health behaviours, WHO

52 EU's Code of Practice on Disinformation

53 Singapore's Protection from Online Falsehoods and Manipulation Act

54 Verified Campaign, United Nations

55 The fight against disinformation and the right to freedom of expression, study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, 2021

56 Verificado, Mexico

57 Notimex, Mexico

58 Observatory of Disinformation and Symbolic Violence on Digital Media and Platforms (NODIO), Argentina

59 Brazilian Internet Freedom, Responsibility, and Transparency Law, Brazil

60 Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, Australia

61 Law 22-20, addressing the use of social media, open broadcast networks, and similar platforms, Morocco

62 Pakistan Electronic Media and Regulatory Authority (PEMRA) Amendment Bill 2023, Pakistan

63 Audiovisual Media Services Directive (AVMSD), 2018

64 Proposition de loi n°388, adoptée par l'Assemblée nationale, en nouvelle lecture, visant à lutter contre les contenus haineux sur internet, France

65 Network Enforcement Act, Germany

66 Italian targeted initiatives to combat specific types of illegal content, Italy

67 California Code, Education Code - EDC § 48900

68 Missouri Revised Statutes Title XI. Education and Libraries § 160.775. Antibullying policy required--definition--content, requirements

69 Criminal Justice (Offences Relating to Information Systems) Act 2017, Ireland

70 Regulations on Minors' Internet Protection, China

REFERENCES

71 Global Threat Assessment

72 Ghana Cyber Security Act 10 (38)

73 International Covenant on Civil and Political Rights (ICCPR)

74 OECD's Privacy Guidelines, 2013

75 Chilean Constitution

76 Data Protection and Privacy Legislation Worldwide

77 American Data Privacy Protection Act (ADPPA)

78 Law No. (13) of 2016 on Protecting Personal Data Privacy, Qatar

79 Data Protection and Privacy Policy (the Policy), Gambia

80 Jordan issues first personal data protection law, Clyde&Co

81 Personal Data Protection Law (PDPL), Oman

82 Personal Data Protection Law, Saudi Arabia

83 Estimated cost of cybercrime worldwide 2017-2028, Statista

84 Verizon DBR report, 2022

85 The European Cybersecurity Index, ESET

86 National Strategy for Cyberspace Security, Portugal

87 Law no. 46/2018, Portugal

88 2020 IBM Report

89 Anti-Cyber Crime Law, Saudi Arabia

90 Electronic Transactions Law, Saudi Arabia

91 Cybercrime law, Rwanda

92 Rwanda inaugurates regional cybercrime investigation centre

93 The disinformation landscape and the lockdown of social platforms, Shawn Walker, Dan Mercea, and Marco Bastos, 2019

94 What is 'digital literacy'?, Douglas A.J. Belshaw, 2011

95 Green Paper: Digital Literacy - 21st Century Competencies for Our Age: The Digital Age, The Fundamental Building Blocks of Digital Literacy - From Enhancement to Transformation, Department of eLearning, 2015

96 World Intellectual Property Organization (WIPO)

REFERENCES

97 European Digital Identity - European Commission

98 Ethics guidelines for trustworthy AI, European Union, 2019

99 Recommendation of the Council on Artificial Intelligence, OECD, 2023

100 DigitalSmarts program, Canada

101 The OECD Privacy Framework, OECD, 2013

102 Digital Dividends, World Development Report, World Bank Group, 2016

103 Guidelines on National Digital Identity, Consultative Committee of Convention the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, 2023

104 https://apolitical.co/solution-articles/en/internet-poverty-connection-mexico

105 https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

106 https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf

107 https://digitalplatformobservatory.org/initiative/charter-of-fundamental-rights-of-digital-labour-in-the-urban-context/#:~:text=The%20Charter%20is%20organised%20around,support%20from%20the%20public%20administration

108 https://www.olartemoure.com/en/bill-artificial-intelligence/

109 https://courier.unesco.org/en/articles/chile-pioneering-protection-neurorights

110 https://www.sydney.edu.au/news-opinion/news/2023/10/24/what-happens-when-technology-learns-to-read-our-minds--.html

111 https://derechodigital.pre.red.es/documentos/CartaDerechosDigitales_04_ENG.pdf

112 https://www.legal500.com/developments/thought-leadership/portuguese-charter-of-human-rights-in-the-digital-age/

113 https://www.japaneselawtranslation.go.jp/en/laws/view/4447/en#:~:text=Article%203The%20formation%20of,to%20participate%20in%20all%20activities

114 https://www.japaneselawtranslation.go.jp/en/laws/view/4276/en#:~:text=Article%201The%20purpose%20of,executing%20administrative%20functions%20under%20its

115 https://www.japaneselawtranslation.go.jp/en/laws/view/4447/en

116 United States Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

117 https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/

118 https://www.infrastructure.gov.au/sites/default/files/documents/acma2023-34431-anonymous.pdf

119 https://www.legislation.gov.au/C2021A00076/latest/text

120 China Global AI Governance Initiative

Digital
Cooperation
Organization

Follow us on

@dcorg | www.dco.org