The impact of digital technology on human rights in Europe and Central Asia

Trends and challenges related to data protection, artificial intelligence and other digital technology issues

Acknowledgements

We would like to thank the researchers of this report, Eimear Farrell and Virginie Martins de Nobrega, for their insights and research, as well as the UNDP Istanbul Hub team including Ainura Bekkoenova, Zana Idrizi, Kubra Ozturk, Mindia Vashakmadze and Maria Vardanyan for their support in the drafting process. The report also benefited from the peer review by UNDP colleagues in Geneva and New York, Roqaya Dhaif and Mirko Ebelshaeuser, as well as Diego Naranja from the European Digital Rights Network. We are grateful for the close collaborations with our country offices and for their inputs and reviews.

We are also thankful for the consultations that were held with thematic national and regional experts, as well as the informal interviews and consultations with many individuals in the countries and territories. We thank for the highly professional work of our editors and layout artists: Andy Quan and Camila Zanzanaini.

Proposed citation

UNDP (United Nations Development Programme) (2023). The impact of digital technology on human rights in Europe and Central Asia: Trends and challenges related to data protection, artificial intelligence and other digital technology issues. Istanbul: United Nations Development Programme.

For more information, contact:

- Ainura Bekkoenova, Policy Specialist on Rule of Law, Security and Human Rights, UNDP Istanbul Regional Hub at ainura.bekkoenova@undp.org.
- Zana Idrizi, Communications, Digital Inclusion and Youth Engagement Analyst, UNDP Istanbul Regional Hub at zana.idrizi@undp.org.
- Kubra Ozturk, Knowledge Management and Partnerships Specialist, UNDP Istanbul Regional Hub at Kubra.ozturk@undp.org.

Contents

Executive summary 1

Introduction 2

1 Trends in digital technology and AI and their impact on data protection, privacy and human rights 4

2 Legislative and institutional frameworks regulating digital technologies and human rights concerns 11

3 Digital transformation and governance of AI 15

4 Specific sectors at higher risk of human rights impacts: a human rights based approach 19

5 Conclusions and recommendations for the adoption and governance of digital technologies and AI based on human rights 21

Addendum to the report: 26

The impact of digital technologies and artificial intelligence on human rights in Europe and Central Asia in 2022

Conclusion 34

Annex A: *International instruments applicable to privacy and data protection* 36

Executive summary

As the use of digital systems accelerated during the COVID-19 pandemic, the scope of 'digital rights' and governance has also developed: moving beyond issues of privacy and freedom of expression to a wider range of issues including algorithmic justice and democratization. Although existing international human rights frameworks can provide some guidance for the use and governance of digital technologies, digital transformation and digitalization, human rights are often left off the agenda.

This study provides an overview of the current situation of the uses of digital technologies, artificial intelligence (AI) and human rights in Europe and Central Asia by exploring regional trends and dynamics, examining national contexts and highlighting common challenges and governance gaps. It investigates how digital technologies are being deployed, used and regulated in the region, with a particular focus on data protection, privacy and AI governance frameworks.

In Europe and Central Asia, there is significant economic and political investment in digital technologies like biometrics, artificial intelligence, video surveillance systems and facial recognition. However, countries in the region have fallen behind in developing a legal framework for privacy and data protection that could address these sophisticated technologies and the needs of society arising from their use. The detailed country reviews show that organizational aspects still need to be fully established and effective implementation, monitoring and evaluation of these mechanisms remain a key challenge.

Across the region, there is a trend towards an increase in unduly restrictive measures, an expansion of censorship and surveillance that threaten the right to privacy, freedom of expression and access to information. While there is a diverse range of experiences and developments across countries in the region, many of them are facing a common set of challenges concerning the regulation and impact of digital technologies and AI, as well as strong pressures on digital human rights and freedoms in the ongoing management of the COVID-19 pandemic.

The review found that in all the countries of Europe and Central Asia, there has been some progress in developing legal frameworks for privacy and data protection, but the implementation of strategic and legal measures tends to lag behind and fails to address the complex outcomes that stem from the use of these technologies. The establishment of adequate oversight and effective regulatory bodies, the encouragement of a law-abiding culture and practices, and the education of citizens and other stakeholders are needed.

Although there are challenges in the uses of digital technologies in the region, the early stage of adopting advanced AI presents a critical opportunity to ensure an inclusive digital transformation that benefits all and respects human rights. The scoping study recommends strategies and commitments to ensure that human rights are protected in practice. The report also presents a set of policy advice for various actors to achieve inclusive digitalization in the region based on human rights.

Introduction

This scoping study proposes a conceptual framework for thinking about the obligations of States and the responsibilities of companies to uphold human rights in line with international standards in the face of States' expanding digital technological capabilities, sometimes referred to as 'digital transformation', in Europe and Central Asia. The study includes recommendations for measures that could be implemented by States, companies, civil society and the international community to ensure that human rights are respected as the power, reach and scope of digital technologies grow.

The first chapter of the study provides a general overview of regional trends and challenges concerning the use and impact of digital technologies and artificial intelligence, analysed through the framework of international human rights law. It includes specific country examples, outlining the categories of human rights that are at risk, and how governments, businesses and civil society organizations are responding to human rights challenges. While recognizing that digital technologies and AI have significant impacts across the whole range of human rights—both online and offline—the study's focus is on freedom of opinion, expression and assembly, the right of access to information, equality and non-discrimination, and the right to privacy and data protection.

The second chapter, 'Legislative and institutional frameworks to regulate digital technologies and human rights concerns', discusses the governance of digital technologies. Its focus is on the European and international legal environment for privacy and data protection, which provides relevant and comprehensive guidance for countries of Europe and Central Asia to develop internal legal and operational frameworks.

The chapter then provides an overview of domestic legal provisions regarding privacy and data protection in Europe and Central Asia, with a short profile of the countries, identifying gaps and developing recommendations for further improvements. The study discusses relevant institutions and policies. Moreover, it equally addresses implementation challenges, including compliance with international standards. Relevant standards are enshrined in the European Union (EU) General Data Protection Regulation (GDPR), the Directive on security of network and information systems (NIS Directive) and the Budapest Convention on Cybercrime. Although these standards do not directly apply in most of the countries of Europe and Central Asia, they influence legal developments in the region.

The third chapter of the study focuses specifically on AI governance and digital transformation in States in the region. Digital transformation has been declared a priority by many States in the region, which have already begun amending existing laws and regulations to support the current wave of digitalization. Nonetheless, challenges arise such as in infrastructure development and digital literacy. While most countries have introduced digital services in various forms to enhance public service delivery, business processes and connectivity, the COVID-19 pandemic, which is associated with a risk of exacerbating existing inequalities, revealed significant gaps in digitalization in countries and territories across the region.

This chapter also identifies industries and sectors exposed to possible risks of adverse impact on human rights by digitalization: the justice sector and law enforcement, health, education and social welfare. It also provides a set of recommendations to carry out human rights impact assessments (HRIAs) in these areas.

The study provides a set of recommendations on the use and governance of digital technologies and AI in Europe and Central Asia, based on human rights, including the identification of strategic entry points and opportunities for UNDP support, engagement and programming. Having moved from a global to a regional perspective on digital transformation, this report proposes a robust human rights framing of digital issues to enable a more sustainable and inclusive digital future that benefits all. The recommendations are directed towards all relevant stakeholders, recognizing that building a responsible ecosystem for digital technologies requires cooperation between the public and private sectors, as well as with academia, media and civil society. The recommendations suggest measures to improve domestic institutional, policy and regulatory frameworks and responses in line with international standards. They are aimed at building a culture of respect and accountability for human rights, democracy and the rule of law in a digital environment. They focus on technical assistance and on developing and disseminating relevant expertise, methodologies and best practices, and facilitating mechanisms for improved transparency and participation by diverse stakeholders. They are also designed to promote regional linkages and international cooperation.

Methodology

The scoping study was commissioned by UNDP, to explore the impact of digital technologies and AI on human rights in Europe and Central Asia. The study defines measures to promote human rights–compliant, people-centred, safe and transparent use of digital technologies and AI in Europe and Central Asia, including recommendations on strategic entry points and opportunities for UNDP's support.

The countries and territories of Europe and Central Asia represent a highly diverse group with distinct subregional development perspectives and challenges, and countries exhibiting heterogeneous levels of digitalization and regulation. The diversity of locations and intricacy of interregional and geopolitical dynamics are important factors. The countries and territories of Europe and Central Asia, divided into subregions, are the following:

- Central Asia (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan)
- The Western Balkans and Türkiye (Albania, Bosnia and Herzegovina, Kosovo,[1] Montenegro, North Macedonia, Serbia and Türkiye)
- South Caucasus and Eastern Europe (Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova, Ukraine)

The study recognizes that these countries and territories are all at different stages of the digitalization process. In some countries, this process is still in its very early stages and the digital divide between urban and rural communities remains significant.

The methodological approach adopted in the scoping study is based on the following elements: a desk-based literature review and comparative analysis of previous research on the topic; a mapping of relevant international and regional initiatives; and an analysis of applicable legal, regulatory and institutional frameworks governing data protection and human rights aspects of the use of digital technologies and AI at the subregional and regional levels. The literature review included academic articles and reports by media, civil society and international organizations, as well as global indexes related to Internet and media freedom, the safety of journalists and human rights defenders, and Internet connectivity and e-government rankings. This research and evidence contributed to informing an understanding of how digital technologies and AI are being used and governed in Europe and Central Asia and how they are perceived to impact, either positively or negatively, on human rights.

Rather than a comprehensive assessment, the analysis has been carried out as a snapshot assessment, given the multi-country approach and constraints related to timing and access and the nature of the virtual dialogue during the COVID-19 pandemic.

1 All references to Kosovo, whether the territory, institutions or the population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 (1999) and without prejudice to the status of Kosovo.

The following key definitions are used in the report:

- **Digitalization:** The application of a wide range of digital tools and technologies to the government, business and consumer [as well as civic] economic and social activities that result in new working arrangements for each.[2]
- **Digital transformation:** Broadly, the organizational transformation enabled by digital technologies and new ways of working. Ure (2021)[3] defines it as the planned promotion and implementation of digitalization across the whole of government, economy and society. In this scoping study, digital transformation is analysed in the context of the national government and regional dynamics.
- **Digital human rights:** Human rights in the context of the use of digital technology and networked spaces.

2 This definition is adapted from John Ure (2021). Digital Solutions Centre in Central Asia. Asia-Pacific Information Superhighway Working Paper Series, No. 07/2021. United Nations ESCAP, 30 August 2021, p. 12. Available at https://unece.org/sites/default/files/2021-10/13E%20Final%20John%20Ure%20DSC%202021_10_18.pdf. UNDP describes digitalization as "the use of digital technologies to change an organization's business model, including creating new or improved ways of delivering services, and improving the quality of what is delivered." See UNDP, UNDP Whole-of-Society Digital Transformation. Available at https://gobiernu.cw/wp-content/uploads/2021/09/UNDP-Whole-of-Society-Digital-Transformation.pdf, p. 4.

3 John Ure (2021). Digital Solutions Centre in Central Asia, p. 13.

1 Trends in digital technology and AI and their impact on data protection, privacy and human rights

This chapter discusses the main issues in societies undergoing digital transformation and examines how specific individual rights are affected by digital technologies.

Global trends

The widespread use of new digital technologies and AI poses both challenges and opportunities for various areas of human rights beyond traditional "digital rights", such as privacy, data protection and freedom of opinion and expression, including freedom of assembly and association.[4] The UN Human Rights Council and the General Assembly confirmed that "the same rights that people have offline must also be protected online";[5] however, many questions remain about the societal consequences of this digital transformation and its impact on human rights. As societies are becoming more dependent on digital technologies, the protection of human rights is ever more critical, as is using these technologies in the public interest.

Digital technologies have transformed the way human rights and freedoms are exercised. The Internet has become crucial for access to information and in the formation of political communities.[6] While the Internet is an indispensable tool for meetings, protests, participation and online campaigns, digital activism is experiencing restrictions on Internet access and communications, digital surveillance, threats to privacy and security, and online censorship. Increased use of digital technologies and AI continues to raise questions around the protection of privacy.[7] Increased online censorship and surveillance threatens "the realization of the principles of transparency and accountability which are essential for the promotion and protection of all human rights, particularly in countries transitioning from autocracy to democracy".[8] While online space facilitates expression and provides for a greater diversity of available information, certain stakeholders have the power to proscribe, remove or distort online content according to their interests.

While AI has a huge untapped potential, unregulated AI design and use have created widely shared concerns over the violation of human rights, especially in terms of discrimination for certain segments of society as a result of "biased algorithms". Studies indicate that "as the use of AI and automated decision-making systems becomes more pervasive, there may be disproportionate and disparate impacts on certain groups facing systemic inequalities, where the algorithms used discrimination against them".[9] The negative impacts of digital technologies on human rights are likely to be highest on those who are already profiled, targeted and harassed in non-digital spaces. It is therefore essential to build bridges between digital rights organizations and other civil society actors, as well as to foster broad alliances between civil society groups and affected communities.

There is a need for a more comprehensive and cross-sectoral approach in addressing the full range of digital human rights challenges to be able to fully benefit from all the positive potential of digital technologies. However, the concomitant threats have become particularly visible during the COVID-19 pandemic, as the use of fast-evolving, advanced digital technologies progressed.

Ultimately, digital technologies alone, especially in a time of crisis, should not be seen as a 'silver bullet' solution to complex issues, for example if the protection of health or upholding public order and safety is at stake. Rather, they should be used as a tool to serve to the benefit of citizens and respond to their needs.

Regional trends

Digital technologies in the region are commonly used for purposes of public safety, law enforcement and State intelligence. Other uses include the use of personal and health data for COVID-19 tracking purposes, using AI for prediction, and employing AI to assist in contact tracing with mobile phone and geolocation data. These new digital technologies have helped governments manage the pandemic and they have played a role in the economic recovery to follow. The region also witnessed the misuse of social media to spread inaccurate information, and the introduction of restrictions on Internet access and on freedom of expression online, i.e. on the Internet.

The COVID-19 crisis has highlighted the need for significant support and investments in digital transformation and effective digital governance across the region, especially to ensure the delivery of core government functions and services. However, there is a lack of comprehensive research addressing the challenges of digital technologies, AI and data processing at a regional level, particularly from a development programming perspective. While there is a diverse range of experiences and variation in levels of development across countries in the region, many of them are facing a common set of challenges in relation to the regulation and impact of digital technologies and AI, as well as strong pressures on digital human rights and freedoms in the ongoing management of the COVID-19 pandemic.

Digitalization offers a chance to improve efficiency, transparency and accountability. However, there are also access and infrastructural challenges, as well as risks of surveillance and other potential threats to human rights. With continued advancements in digitalization, the risk of increasing the rural-urban divide is deepening along with the increased risk of alienation of population groups without access to digital technologies and services. Given the central role digital technologies play in gaining access to resources, jobs, health care, education and public services, the digital divide is increasingly acknowledged as a human rights issue. It is important to "leave no one behind" in technological progress, as expressed by the United Nations 2030 Agenda for Sustainable Development. As access to the Internet has become even more critical during the COVID-19 pandemic, States should work to ensure the broadest possible access to Internet service by taking steps to bridge digital divides, including the gender digital divide. As States are announcing their ambitions for AI and digital transformation, it is imperative they consider societal needs, as well as the human rights implications of the use of digital technologies and AI.

Freedom of expression and access to the Internet

According to 'Freedom on the Net', Internet freedom declined worldwide in 2021 for the 11th consecutive year, including in the countries assessed by the Freedom on Net Report as shown below (Table 1).[10] The trend is also true for the region with the persisting struggles for open and fair access to the Internet and freedom of expression. In the backdrop of COVID-19, freedom of expression online is subject to unprecedented strain, with more governments than ever before suspending Internet access, blocking social media platforms, and filtering or restricting online content.

Deterioration of Internet freedom was documented in several countries in Europe and Central Asia, including Uzbekistan and Belarus.[11] The combination of political polarization and technological change has resulted in the rapid spread of hate speech, misogyny and inaccurate information, often leading to disproportionate restrictions on freedom of opinion and expression.

Freedom on the Net 2021 – ECIS Regional Score

Global Rank	Regional Rank	Country	Status	A	B	C	Total
9	1	Georgia	F	19	31	27	77
16	2	Armenia	F	19	26	26	71
17	3	Serbia	F	21	25	25	71
35	4	Kyrgyzstan	PF	13	23	17	53
52	5	Azerbaijan	NF	10	14	11	35
53	6	Türkiye	NF	15	10	9	34
54	7	Kazakhstan	NF	11	11	11	33
56	8	Belarus	NF	10	14	7	31
59	9	Uzbekistan	NF	9	12	7	28

Key

F = Free, PF = Partly Free, NF = Not Free

A = aggregate score for A. Obstacles to Access (0–25 points) category

B = aggregate score for B. Limits on Content (0–35 points) category

C = aggregate score for C. Violations of User Rights (0–40) category

Total = aggregate score for all categories

A combined score of:

70–100 = Free

40–69 = Partly Free

0–39 = Not Free

Source: Adapted from Freedom on the Net 2021

4 See Office of the UN High Commissioner for Human Rights, A/HRC/20/27, para. 84 (k).

5 See Council resolutions 20/8 and 26/13 and UN General Assembly resolution 71/199.

6 A/HRC/17/27, paras. 2 and 19; A/HRC/23/50, para. 15.

7 The United Nations General Assembly, the United Nations High Commissioner for Human Rights and several other UN human rights mechanisms have recognized privacy as a 'gateway' right and a prerequisite for the full exercise of other human rights (UN General Assembly resolution 68/167; A/HRC/13/37; A/HRC/29/32. See also Human Rights Council resolution 20/8.)

8 Office of The United Nations High Commissioner For Human Rights (2007). "Good Governance Practices for the Protection of Human Rights", available at: https://www.ohchr.org/sites/default/files/Documents/Publications/GoodGovernance.pdf

9 Solon Barocas and Andrew D. Selbst, "Big data's disparate impact", California Law Review, vol. 104 (2016); Danah Boyd, Karen Levy and Alice Marwick, "The networked nature of algorithmic discrimination", in Data and Discrimination: Collected Essays, Seeta Peña Gangadharan, Virginia Eubanks and Solon Barocas, eds. (2014).

10 'Freedom on the Net' is produced annually by Freedom House, a pro-democracy think tank. Performance is analysed according to three criteria: Obstacles to Access (A); Limits on Content (B); and Violations of User Rights (C) For the 2021 edition, see Freedom House, Freedom on the Net 2021, available at https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf, Full rankings and methodology are available at: https://freedomhouse.org/report/freedom-net.

11 Ibid., p. 1.

Crisis responses to COVID-19 exacerbated the deterioration of Internet freedom by governments in the region. This was due to the exploitation of emergency laws, COVID-19 related restrictions and weak data protection laws which resulted in the expansion of censorship and surveillance. Many civil society organizations (CSOs) are concerned that the 'temporary' emergency measures introduced during the pandemic period could become permanent "because in moments of crisis there's a deeper allowance in terms of public trust and legal authority."[12] According to Article 21 of the International Covenant on Civil and Political Rights (ICCPR), governments can restrict citizens' rights to protect public health. However, this permission is only granted under standards of necessity and proportionality.[13] In various countries, the COVID-19 pandemic measures have been used to justify the suppression of critical speech online and to censor politically unfavourable content without meeting the high standards of necessity in line with the ICCPR.

The UN Human Rights Council condemns unequivocally any measures in violation of international human rights law to prevent or disrupt access to, or the dissemination of, information online.[14] Full access to the Internet and digital communication platforms should be realized by governments as this is essential to ensure citizens' access to public services as well as to relevant information.[15]

Similar to other parts of the world, Internet shutdowns in Europe and Central Asia have been used to restrict access to information, often in the context of an election, or during a political conflict or public protests.[16] Shutdowns can broadly be defined as 'the intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information' . More specifically, it can be defined as the 'measures taken by a government, or on behalf of a government, to intentionally disrupt access to, and the use of, information and communications systems online. During elections, some governments blocked various social media channels in an attempt to disrupt access to information.[17] Internet shutdowns not only disrupt communication and access to information, but in the context of an election can also hinder the realization of the right to political participation and may have wider effects on society and democracy as a whole.

As stated by the UN Secretary-General in his Roadmap for Digital Cooperation, "States and business enterprises in the region should ensure transparent and accountable content governance frameworks that protect freedom of expression, avoid incentives for overly restrictive moderation practices and protect the most vulnerable".[18] In many countries in Europe and Central Asia, journalists and online bloggers are reported to face physical and verbal attacks that threaten their ability to report news and information to the public. They may face arrest for non-violent political, social or religious speech.

Blanket Internet shutdowns and generic blocking and filtering of services are considered by UN human rights mechanisms to be in violation of international human rights law.[19] Internet access is crucial for protecting people's right to access information. Therefore, States need to end existing Internet disruptions or shutdowns and ensure affected people stay connected to the Internet. There are already CSOs actively monitoring the situation in the region. For example, the "Pandemic Big Brother" project has monitored legislative changes and other trends affecting human rights in the digital sphere across several countries in the region during the pandemic period.[20]

COVID-19, access to accurate information and freedom of expression

As many activities shifted online during the pandemic, the public sphere became polluted with content designed to manipulate and misinform citizens, which disrupted access to accurate information about COVID-19. According to UNESCO and UNITAR, "Falsehoods and misinformation have proven deadly and sowed confusion about life-saving personal and policy choices". Several governments in the region, such as those of Ukraine and Georgia, with support from UNDP have worked on innovative ways to stop the spread of false information flow in the region and to reduce the reach and impact of this flow on public health. However, in some countries and territories[21] in the region, governments are still resorting to restricting information and censorship to fight misinformation related to COVID-19.

Although accurate data and information related to the virus is fundamental for an effective response, public health emergency powers should not be used to limit access to information, restrict content or prevent criticism of government policies, to shut down the Internet or impose technical controls, or to silence the work of human rights defenders or journalists. Journalists, civil society activists, human rights defenders and members of the general public have faced attacks, including online abuse, trolling, smear campaigns and pressure to retract content.

According to the UN human rights office, the Inter-American Commission for Human Rights, and the Organisation for Security and Co-operation in Europe (OSCE), penalizing expressions based on vague concepts such as fake news or disinformation in relation to the COVID-19 pandemic are not compatible with the requirements of legality and proportionality—and it is disproportionate and illegitimate in all cases due to its outsized negative effect on society.[22] The human right to impart information and ideas is not limited to "correct" statements, and "States are under a positive obligation to foster an enabling environment for freedom of expression, which includes promoting, protecting and supporting diverse media".[23]

Apart from spreading hate, social media platforms are often exploited to propagate disinformation, misinformation and propaganda, including in the context of elections, where they are designed to manipulate voting and support efforts to sabotage democratic processes, thereby undermining not only individual human rights but also collectively influencing democracy and society as a whole. AI-driven systems can contribute to the restriction of online freedom of assembly through targeted blocking of content on online platforms, which silences already marginalized and vulnerable communities. The spread of such content is a core challenge facing States given that its malignant use can mislead people and serve to undermine human rights and democracy. This is especially true in fragile democracies and regions experiencing conflict, as well as in the context of the COVID-19 pandemic, where citizens may struggle to access high-quality, accurate information.

There has also been a shift away from trying to control the behaviour of individual perpetrators of online hate and misinformation, and a move instead towards holding platforms responsible for the material they display. This has mainly focused on social media companies and asks them to hold perpetrators responsible by, for example, blocking or deleting accounts. This has created a shift in responsibility from the government or individuals to the platforms by making them the point of contact for complaints. The question of social media liability has raised a wider debate about the responsibility of Internet companies more generally, which have, until now, enjoyed little or no regulation. With the movement away from self-regulation and voluntary codes (e.g. the 2016 EU Voluntary Code of Conduct) to greater State regulation of the Internet and social media through legal norms (e.g. the EU Digital Services package), many States are currently grappling with this controversial issue, and it is an area that is still very much in development.

According to various transparency reports by some of the major social media companies, there is a relatively large number of information requests and content restriction requests by States in Europe and Central Asia, with the Turkish government ranking in seventh place globally for user data requests submitted to Facebook in 2020.[24]

Privacy rights and data protection are also important concerns in this context, with an increase in the use of COVID-19 tracking applications, collection and monitoring of user data, often without consent, especially as smartphone apps for contact tracing, vaccine management and quarantine compliance are deployed with few safeguards against abuse.

Although the use of digital technologies and AI helped governments manage the pandemic, they also raised debate around the impact of these technologies on human rights. While the information collected by these apps may be justified and useful in certain cases, it is important that authorities exercise proportionality and transparency while respecting privacy and data protection. The use of digital tools for citizen surveillance by some countries in the region is unfortunately common and there is a need to introduce safeguards and checks and balances in the government policies regarding digitalization.

As advocated by the European Center for Not-for-Profit Law (ECNL), CSOs must be proactively involved in the creation of digitalization policies as the involvement of civil society brings expertise and real-life examples about the impact of digitalization and AI-based systems on different groups of people, including risks to human rights.[25] In a joint statement on digital contact tracing, the chair of the Committee of the Convention 108 and the data protection commissioner of the Council of Europe (CoE) highlighted several guiding principles, such as transparency of data collection, use and storage; oversight and audit; anonymization; and impact assessment.[26] The involvement of relevant stakeholders like civil society would contribute to the rights-respecting use and deployment of AI and build trust in the use of AI systems throughout societies.

While new technologies have helped civil society networks to grow and have created a space for exchange, mobilization and participation, they have also given authorities excuses to control civil society movements and curtail media freedoms, often under security pretexts. During the past few years, there has been a widespread deterioration in the conditions for civic space both across the globe and online. The pandemic has exacerbated these trends, posing greater challenges for fundamental freedoms such as freedom of assembly and association.[27]

Many human rights defenders in the region are increasingly subjected to surveillance and reprisals, and to violation of their privacy, often under the justification of fighting terrorism or extremism. Particularly with the increased presence of information online in electronic systems and databases, digital threats to human rights are increasingly common, and surveillance and hacking have

12 Cited in Victoria Kim, "Who's Watching? How Governments used the pandemic to normalize surveillance", Los Angeles Times, 9 December 2021, available at https://www.latimes.com/world-nation/story/2021-12-09/the-pandemic-brought-heightened-surveillance-to-save-lives-is-it-here-to-stay.

13 United Nations (General Assembly). (1966). International Covenant on Civil and Political Rights. Treaty Series, 999, 171.

14 See Human Rights Council Resolution, The promotion, protection and enjoyment of human rights on the Internet, adopted 17 July 2018, A/HRC/RES/38/7.

15 OHCHR, COVID-19 Guidance (13 May 2020), available at https://www.ohchr.org/Documents/Events/COVID-19_Guidance.pdf.

16 OHCHR, "Internet Shutdowns and Human Rights", April 2021, available at https://www.ohchr.org/Documents/Press/Internet-shutdowns-and-human-rights.pdf.

17 Yan Auseyushkin and Andrew Roth. "Will knocking Belarus offline save president from protests?" The Guardian, 11 August 2020, available at https://www.theguardian.com/world/2020/aug/11/belarus-president-cuts-off-internet-amid-widespread-protests.

18 United Nations (2020). Report of the Secretary-General Roadmap for Digital Cooperation. Available at https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

19 Ibid., p. 14.

20 Similarly, the "COVID-19 Civic Freedom Tracker" is run as a collaborative effort by the International Center for Not-for-Profit Law (ICNL) and the European Center for Not-for-Profit law (ECNL): ICNL, COVID-19 Civic Freedom Tracker, available at https://www.icnl.org/covid19tracker/

21 UNDP (2022). Mapping of Initiatives to Counter Information Pollution in Europe and Central Asia Region. November. Available at https://www.undp.org/eurasia/publications/information-pollution

22 OHCHR, COVID-19 Guidance (13 May 2020), available at https://www.ohchr.org/Documents/Events/COVID-19_Guidance.pdf, Organization for Security and Co-operation in Europe (OSCE), "COVID-19: Governments must promote and protect access to and free flow of information during pandemic, say international media freedom experts", 19 March 2020, available at https://www.osce.org/representative-on-freedom-of-media/448849.

23 OHCHR, OSCE, OAS and ACHPR, "Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda", 3 March 2017, FOM.GAL/3/17, available at https://www.osce.org/files/f/documents/6/8/302796.pdf.

24 Facebook's Global Government Requests Report provides transparency about the number of government requests related to obtaining user data, restricting content, national security and violations of local law. In January to June 2021, Türkiye submitted 7,825 requests, for which some data were disclosed in 59% of cases. See https://transparency.fb.com/data/government-data-requests/country/TR/. Twitter's Information Requests Report similarly provides insights into legal demands to produce account information from governments and law enforcement. See https://transparency.twitter.com/en/reports/information-requests.html#2020-jul-dec.

25 ECNL, "Country papers on participatory processes in drafting national AI policies in the Czech Republic, the Netherlands, Australia and Canada", 19 April 2021, available at https://ecnl.org/publications/being-ai-ware-incorporating-civil-society-national-strategies-artificial-intelligence.

26 Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 28 April 2020, available at https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7.

27 Secretary General's Roadmap for Digitalization. 2020. Available at: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

grown in scope and complexity.

The issues raised include not just surveillance but also the production of structural discrimination and inequalities. For example, there have been concerns regarding the disparate impact of AI and digital surveillance on populations that are already discriminated against by police, e.g. marginalized and minority groups, as predictive policing tools end up factoring in data reflecting conscious and implicit bias.[28]

The use of digital tools and AI for law enforcement and its impact on human rights

Several countries in the region have been using AI and biometrics technologies for law enforcement, security and COVID-19 tracking. Since AI often relies on personal data to operate, the rights to privacy and data protection are severely affected by the various uses of these technologies. Uses of biometric technologies, which include facial recognition, can potentially allow unlimited tracking of individuals. If not properly regulated, the use of AI and biometrics technologies can amplify structural inequalities as certain populations, such as racial minorities, may be at greater risk of human rights violations in relation to pandemic surveillance.[29]

The recent UN Report on digitalization outlines the human rights risks and implications of the widespread use of AI by governments and businesses, human rights impacts of AI systems which are beyond threats to the individual right to privacy.[30] As the report observes, "deeply intertwined with the question of privacy are various impacts on the enjoyment of other rights, such as the rights to health, education, freedom of movement, freedom of peaceful assembly, freedom of association and freedom of expression."[31] The report also notes the inadequacy of existing data protection and privacy laws that focus on personal data as "AI systems do not exclusively rely on the processing of personal data … [and] even when personal data are not involved, human rights, including the right to privacy, may still be adversely affected by their use."[32] This emphasis on economic, social and cultural rights, such as rights to health and education and the right to work, is of critical importance, particularly in relation to the increasing use of AI in public services. The issues raised include not just surveillance but the production of structural discrimination and inequalities.

28 Rashida Richardson, Jason M. Schultz, and Kate Crawford. "Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice." NYUL Rev. Online 94 (2019), p. 15. Available at https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf.

29 Tereza Hendl, Ryoa Chung and Verina Wild. "Pandemic surveillance and racialized subpopulations: mitigating vulnerabilities in COVID-19 apps." Journal of bioethical inquiry 17, no. 4 (2020), pp. 829–834. Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7445800/.

30 UN High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/48/31. 13 September 21.

31 Ibid., Section I, article 3.

32 Ibid., Section III, A, article 15.

Central Asia

Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan

Most of Central Asia still faces challenges in ensuring good digital connectivity and enabling people to benefit fully from digitalization and digital transformation. Nearly half of the population in Central Asia is not digitally connected, and even when available, an Internet connection is often expensive and of poor quality.[33] Global rankings of the state of digital and network readiness show Kazakhstan as a digital leader, significantly ahead of the other Central Asian countries, followed by Uzbekistan then Kyrgyzstan.[34] Tajikistan and Turkmenistan fall below the global average in terms of the number of individuals using the Internet.[35] In the latest UN Global E-government Survey 2020, which measures online public services, information and communications technology (ICT) infrastructure, and human capital, Kazakhstan appears in the highest-ranking group at 29th place globally and Kyrgyzstan also scores relatively well.[36]

In response to the recent COVID-19 pandemic, governments in Central Asia demonstrated an ability to move quickly, when necessary, from improving access to digital government services to setting up call centres and hotlines and launching information platforms. But there is a need for further public sector efforts in digital skills development, policy reforms and improving data protection and cybersecurity. Public awareness of digital rights and the impact of digitalization is low. Corruption, particularly within law enforcement agencies, as well as weak legislative and judicial bodies, continue to have a deleterious impact on the effective realisation of human rights.

During the pandemic, 'fake' news and misinformation about COVID-19 was spread widely through social media in Central Asia. In many cases, States responded by introducing new laws that threatened restricting freedom of expression online. While Central Asian governments have adopted various approaches, it can be observed that the protection of human rights online has generally deteriorated across the region.

As described previously, according to the Internet freedom scores from Freedom House, only Kyrgyzstan among the countries of Central Asia is ranked "partly free" for Internet openness and both Uzbekistan and Kazakhstan are considered "not free."[37] While not included in the annual Freedom on the Net survey, Freedom House reports elsewhere that Tajikistan and Turkmenistan have used blackouts of news portals and social media platforms to suppress potential anti-government criticism and opposition.[38]

Some commentators have pointed to a growing trend among Central Asian countries of testing how far they can go to restrict Internet freedoms.[39] There is a sense that digital transformation in Central Asian countries is primarily State-centred rather than people-centred. There is significant investment in the region by private sector technology companies from China (e.g. Huawei) and Russia, leading to monopolies, outsourcing of data management and concerns about possible surveillance.[40] Surveillance technologies may be initially introduced for reasons such as keeping citizens safe or improving road security, but privacy questions arise over who has access to and stores the data, and for what purposes.

Governments in Central Asia need to develop a more sustainable digital ecosystem. This includes investment in increasing access to digital devices, enhancing local content, and developing the digital skills and resilience of the population. To reap the full spectrum of benefits offered by the digital world, Central Asian countries will also need to build trust among citizens by boosting cybersecurity, data protection and protecting human rights online. Given that some countries in Central Asia are still in the early stages of digital transition, there is a significant opportunity to ensure inclusive digital transformation that benefits all and respects human rights.

Multilateral bodies such as the United Nations and the EU have a key role to play. In 2019, the EU adopted a new strategy on Central Asia within which education is one of the main areas of cooperation.[41] Through this mechanism, the EU and Central Asia are cooperating to support the development and maintenance of high-capacity research and education networks; promoting digital literacy and skills; fostering digital entrepreneurship and job creation; and developing areas such as e-government and e-education.

Among other multilateral and bilateral donors and international development agencies, the World Bank runs a regional Digital Central Asia–South Asia programme (Digital CASA),[42] the aim of which is to help bring reliable and affordable Internet services to the region and catalyse innovations in the delivery of public and private services. The Asian Development Bank and the Japanese government also operate digital development programmes in the region.

33 Lilia Burunciuc, "How Central Asia can ensure it doesn't miss out on a digital future", World Bank Blogs, 21 June 2021, available at https://blogs.worldbank.org/europeandcentralasia/how-central-asia-can-ensure-it-doesnt-miss-out-digital-future.

34 See Portulans Institute, The Network Readiness Index 2020, Soumitra Dutta and Bruno Lanvin, eds., available https://networkreadinessindex.org/2020/wp-content/uploads/2020/11/NRI-2020-V8_28-11-2020.pdf; International Telecommunications Union, Measuring digital development: Facts and figures 2021, available at https://www.itu.int/itu-d/reports/statistics/facts-figures-2021/.

35 UN DESA, E-Government Survey 2020, Digital Government in the Decade of Action for Sustainable Development (2020), p. 66, available at https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020.

36 Ibid., see Table 2.8, p. 58 and Table 2.3, p. 48.

37 Scores available at Freedom House, Freedom on the Net, "Countries", available at https://freedomhouse.org/countries/freedom-net/scores.

38 Freedom House, Freedom in the World 2021, see country reports on Turkmenistan and Tajikistan, section D1, https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege/countries-and-regions.

39 Isabelle Khurshudyan, "Central Asian leaders want to tighten grip on social media. Russia's playbook blazes the trail", Washington Post, 7 November 2021, available at https://www.washingtonpost.com/world/asia_pacific/uzbekistan-kazakhstan-big-tech/2021/11/06/857efe86-3db4-11ec-bd6f-da376f47304e_story.html.

40 Bradley Jardine, "China's Surveillance State Has Eyes on Central Asia", Foreign Policy, 15 November 2019, available at https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/. Also see Steven Feldstein, The Global Expansion of AI Surveillance, Working Paper, Carnegie Endowment for International Peace, September 2019, available at https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

41 European Union, "EU Builds a Strong and Modern Partnership with Central Asia: Central Asia Fact Sheet", undated, available at https://eeas.europa.eu/sites/default/files/factsheet_centralasia_2019.pdf.

42 Juan Navas-Sabater, World Bank regional digital programs in Central Asia: The example of the Digital CASA regional program. Presentation. UNESCAP Expert group Meeting on the Asia-Pacific Information Superhighway in North and Central Asia, 31 January 2019, Almaty, Kazakhstan, available at https://www.unescap.org/sites/default/files/The%20example%20of%20the%20Digital%20CASA%20regional%20program%2C%20World%20Bank.pdf.

South Caucasus and Eastern Europe

Armenia, Azerbaijan, Georgia, Belarus, Republic of Moldova, Ukraine

As part of the management of COVID-19, many governments in Europe and Central Asia applied restrictive measures to the use of the Internet and digital technologies, impacting adversely on human rights and civic freedoms. This trend was reflected in the Eastern Partnership region, where countries piloted an array of emergency measures, including restrictions on the distribution of health-related 'fake news', often threatening freedom of expression and access to information.[43] In some countries including Armenia and Belarus, such measures inhibited people from accessing valuable information related to how the State is handling the emergency situation. There were also limitations imposed on journalists on posting news.

States introduced measures that negatively affected the privacy of individuals. Three countries (Armenia, Georgia and Ukraine) introduced contact tracing apps. Armenia also adopted legal measures that allow authorities to collect information on the location and calls of the users of electronic communication services to trace contacts of potentially infected people during the period of the state of emergency.

Digital technologies were also used to facilitate access to human rights, for example the right to freedom of assembly. During the pandemic period, there was an increase in the use of digital technologies in the region to hold online assemblies, as well as to assist the organization of assemblies on the ground. For example, in the Republic of Moldova a flash mob took place on Facebook for World Press Freedom Day and in Belarus two annual marches that were cancelled in Minsk (Freedom Day on 25 March and "Chernobyl's Road" on 26 April) took place online instead. The first ever online rally in Belarus was organized on 1 May by the former chairman of the United Civil Party, Anatoly Lyabedzka, receiving over 10,000 views.[44]

Since the outbreak of the COVID-19 pandemic, digital technologies have also been seen as essential to delivering the right to work and the right to education though the provision and effective continuation of online education and teleworking. In terms of Internet access and digital literacy, the EU-funded Eastern Partnership Civil Society Forum has examined the prevalence of digital literacy across the Eastern Partnership (EaP) region and recommended that EaP governments improve ICT infrastructure, particularly in rural and remote areas and conflict regions, and provide training and information campaigns to increase people's digital literacy.[45]

43 April Gordon, "In Eastern Europe and Beyond, a Dearth of Guidance on Regulating Disinformation", Perspectives, Freedom House, 8 July 2020, available at https://freedomhouse.org/article/eastern-europe-and-beyond-dearth-guidance-regulating-disinformation.

44 ECNL, One Year of COVID-19: Emergency Measures and Civic Freedoms in the Eastern Partnership Region, April 2021, available at https://ecnl.org/sites/default/files/2021-04/EaP%20Emergency%20Measures%202021%20April%20final.pdf.

45 Eastern Partnership Civil Society Forum, Digital Literacy in times of the COVID-19 in the Eastern Partnership Countries (2021), available at https://ecnl.org/sites/default/files/2021-04/EaP%20Emergency%20Measures%202021%20April%20final.pdf.

The Western Balkans and Türkiye

Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia and Türkiye

The Western Balkans and Türkiye enjoy good connectivity as the majority of the population has access to digital devices and the Internet. There are also many digital public services available for citizens. The possibility of EU accession has prompted a variety of positive legislative and policy reforms across this subregion during the last few years, including in the digital sphere. However, within the fragile democracies of the Western Balkans, a rapid growth in telecommunication and computing technology has emerged alongside low levels of media literacy and a widespread lack of information on data privacy, as well as immature institutions that may be prone to misusing the data, and a lack of effective implementation of data protection laws.

The COVID-19 pandemic brought some negative developments in terms of human rights in the digital sphere. During 2019 and 2020, two of the leading CSOs dealing with digital rights in the region, the Balkan Investigative Reporting Network (BIRN) and the SHARE Foundation, published a series of reports documenting a rise in digital rights violations, with over half of the cases involving manipulation of the digital environment, including propaganda, disinformation and the publication of unverified and inaccurate information. They verified more than 800 violations of digital rights overall "including violations of privacy and data protection, censorship and efforts to prevent legitimate speech, as well as attempts to overwhelm users with misinformation and discriminatory or derogatory content, often for financial or political gain".[46]

Many interviewees for this scoping study revealed that, beyond specialized CSOs working on digital rights within the countries covered, there seems to be little awareness or understanding among the general public in the region of what constitutes digital human rights. There is also a paucity of information regarding the impact of digital technologies on society in local media. Furthermore, civil society interviewees mentioned difficulties in engaging with public authorities on the topic of human rights and digital technologies, especially in relation to specific sectoral legislative initiatives such as on policing. The previously mentioned report by BIRN and SHARE stresses that "those guilty of using the digital space to undermine democracy, intimidate others from publishing the truth or to spread malicious falsehoods operate with impunity, not least because there is no meaningful sense in the region of what constitutes digital rights—never mind the desire to or means to protect those rights".[47]

Pressure on journalists is a major obstacle for media freedom in the Western Balkans and Türkiye, with threats and attacks on journalists leading to self-censorship. Online attacks seem to have risen in the region and this may be due at least in part to the COVID-19 pandemic, which has made people more dependent on the Internet and on social media as a key forum for public debate. Social media platforms are plagued by an increasing level of disinformation, abusive content and hate speech. Moreover, the COVID-19 pandemic outbreak has been accompanied by a rapid spread of false health advice, triggering conspiracy theories related to the vaccines, the causes of the pandemic and how the virus is spread. Many of these theories had political connotations or stoked ethnic tensions by blaming particular communities or nationalities. The situation requires a broader regional lens as disinformation on the pandemic is not restricted to national borders. In terms of positive responses, several organizations in the subregion are involved in fact-checking initiatives.

A lack of accountability among big tech companies and platforms remains a key issue in the region. Some civil society actors have expressed concerns about the relationship Big Tech companies enjoy with certain governments in the region. Only Google and Viber have appointed official representatives to the region, while others maintain representative offices that cover all of Europe or Central Europe. The lack of local representation and language skills, as well as a lack of clarity over jurisdiction, can result in errors and delays for content removal decisions by social media platforms, while the public is left with limited access to this media.

Civil society interviewees cited the need to build a broad coalition of stakeholders in the region to raise public awareness on human rights relating to digital technologies. At the same time, they acknowledge this is a complex issue, and that further dialogue, research and advocacy are needed on what type of actions may be necessary to promote and safeguard these rights. A number of encouraging civil society efforts are already making progress in this area. For example, a Digital Rights Network for Southeast Europe was established in 2020 to connect civil society organizations across the region and build capacity.[48] Several of the major CSOs working on digital rights in the region have launched "Platform B: Amplifying Strong and Credible SEE Voices", an online platform and event series.[49] Selected CSOs are being supported to conduct "Digital Agenda Advocacy Initiatives" by an EU-funded project on "Increasing Civic Engagement in the Digital Agenda (ICEDA)"; its aim is to establish an informal network of CSOs and media from the Western Balkans to promote dialogue, digital literacy, skills and inclusion.[50] And a media literacy campaign, OpisMEDIJavanje ("learning about media literacy"), has been spearheaded by Kosovo-Albanian and Kosovo-Serbian journalists.

46 BIRN and Share Foundation, Digital Rights Falter Amid Political Unrest (2021), available at https://balkaninsight.com/wp-content/uploads/2021/07/Digital-Rights-Falter-Amid-Political-and-Social-Unrest-Report.pdf; also see Civitates, Share Foundation and BIRN, Pandemic for Digital Rights: South East Europe Report, available at https://bird.tools/wp-content/uploads/2020/11/Pandemic-for-Digital-Rights-2020.pdf.

47 BIRN and SHARE Foundation, Digital Rights Falter amid Political and Social Unrest (2021), p. 8, available at https://balkaninsight.com/wp-content/uploads/2021/07/Digital-Rights-Falter-Amid-Political-and-Social-Unrest-Report.pdf.

48 BIRN, "SEE Digital Rights Network Established", BalkanInsight, 31 August 2020, available at https://balkaninsight.com/2020/08/31/see-digital-rights-network-established-2/.

49 BIRN Investigative Resource Desk, "Platform B: Amplifying Strong and Credible SEE Voices", event announcement, 23 June 2021, available at https://bird.tools/platform-b-amplifying-strong-and-credible-see-voices/.

50 Metamorphosis, "Increasing Civic Engagement in the Digital Agenda – ICEDA", 21 February 2020, available at https://metamorphosis.org.mk/en/proekti_arhiva/increasing-civic-engagement-in-the-digital-agenda-iceda/; also see Metamorphosis, "Regional Dialogues for the Digital Agenda: Artificial Intelligence and Algorithms in government e-services, held in Belgrade", 15 July 2021, available at https://metamorphosis.org.mk/en/aktivnosti_arhiva/regional-dialogues-for-the-digital-agenda-artificial-intelligence-and-algorithms-in-government-e-services-held-in-belgrade/.

2 Legislative and institutional frameworks regulating digital technologies and human rights concerns

Global overview

Various regulatory frameworks are relevant in terms of governance of the digital sphere, including artificial intelligence. The applicable legal instruments include international law, regional treaties, national constitutions and domestic law pertaining to human rights, data protection, cybersecurity, intellectual property (IP), trade, company law, media law, consumer law and safety, international humanitarian law, health law and environmental law, among others.[51] International law, including international human rights law, applicable to data protection and privacy, provides an overarching framework for regulation in the area of digital technologies and AI. There are comprehensive multilateral treaties that provide for regulation of cross-border data flows, and the safeguards of the right to privacy and the protection of individuals' personal data. Various international organizations, including the EU, the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe, have sought to develop international standards governing data protection, privacy and cross-border data flows. An overview of the main international instruments in this domain is provided in Annex A.

While bringing substantial benefits to individuals and society, digital technologies and AI systems also pose certain risks and may have a negative impact on human rights including the application of facial recognition systems for mass surveillance, algorithmic bias, lack of transparency resulting in lack of fairness, lack of privacy, data misuse and in deepfakes spreading misinformation. From calls for greater regulation of facial recognition systems to policies designed to prevent AI-driven automation from exacerbating labour market inequality, a growing number of countries and organizations are trying to articulate principles by which AI can be prevented from causing harm.

Within Europe and Central Asia, the prospect of EU integration has proved an effective tool for the harmonization of legislation. As part of their accession, the EU Enlargement and Integration countries included in this study are expected to align their data protection laws with the EU General Data Protection Regulation ("GDPR"), which grants rights to individuals to control personal data and creates specific new data protection requirements.[52] These candidate and potential candidate countries and territories are Albania, Bosnia and Herzegovina, North Macedonia, Kosovo, Moldova, Montenegro, Serbia, Türkiye and Ukraine. European neighbourhood policy countries associated with Horizon 2020 are Armenia, Georgia and Tunisia. It is further worth noting that the GDPR includes provisions that carry extraterritorial implications of relevance for all countries considered in this study, particularly in the context of transborder data flows because GDPR applies to entities outside the EU that offer goods or services (for payment or for free) to individuals in the EU or that monitor the behaviour of individuals in the EU.[53]

The following countries of Europe and Central Asia are members of the Council of Europe and, as such, are likely to be influenced by the relevant principles promoted by the Council of Europe: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Montenegro, North Macedonia, the Republic of Moldova, Serbia, Türkiye and Ukraine. While Türkiye is the only OECD member among Europe and Central Asia, the OECD nevertheless wields a normative and economic power extending beyond its immediate membership.

While on a formal level, countries in the region seem to be progressing with developing the necessary national legislative and administrative environments, there is a gap evident in the implementation of the prescribed measures. The European Commission, which has the power to determine whether a country outside the EU offers an adequate level of data protection to the GDPR, has not yet recognized any of the countries of Europe and Central Asia as providing such protection.[54] The countries under consideration in this study should also take into consideration recent legislative developments in the EU, including proposals for a Digital Services Act and a Data Governance Act, which could lead them to be able to further harmonize their legal systems with the EU law.

51 The UNCTAD Global Cyberlaw Tracker is a useful resource for tracking the state of legislation in the field of e-transactions, consumer protection, data protection and privacy, and cybercrime. See UNCTAD, "Summary of Adoption of E-Commerce Legislation Worldwide", available at https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

52 European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj.

53 See further: European Commission, "Rules on international data transfers", available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en.

54 European Commission, "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection", available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Regional overview

Governments in the region are scaling up their capacities to apply digital technologies in economic, social and other areas. However, the need for robust data governance is not adequately perceived. Human rights risks and benefits driven by digital technologies, which affect people and communities, sometimes in unforeseen or unintended ways, need to be addressed and regulated.

Legal frameworks governing data protection and privacy

The domestic legal provisions in the study countries are clearly influenced by international standards and mechanisms on privacy and data protection, especially where those countries are members, prospective members or partners of relevant international organizations. There is some progress in establishing both legal and operational frameworks for privacy and data protection in most of the study countries. Nevertheless, while transposing international agreements and standards into national laws is an important albeit first step, equally important is the implementation of legislation, which requires political will, cultural change and capacity-building, as well as the establishment of independent and effective oversight mechanisms. Institutions responsible for effective implementation should be introduced and strengthened. It is also crucial to raise awareness among citizens.

Within the subregions covered in this report (South Caucasus and Eastern Europe, Western Balkans and Türkiye, and Central Asia), there are heightened risks to data protection and the privacy of individuals due to reasons such as the acceleration of change driven by innovation in the technological environment, the globalization of the world economy, greater direct participation of citizens in data transfers, and the ubiquity of the Internet and online services. However, notwithstanding these fundamental changes in the data collection, processing and retention landscape, progress in the advancement of regulation, oversight and enforcement of data protection and privacy, both domestically, regionally and across borders, has moved relatively slowly.

Regarding the legal frameworks in the various jurisdictions, and with respect to data protection law in particular, this scoping study has found that legislative frameworks have been subject to ongoing revision and development. However, examination of individual countries in the region clearly highlights the wide variance in the importance assigned to this process by the respective legislatures.

While the data protection and privacy laws in Europe and Central Asia share many of the same core elements, they each have their own specific rules and mechanisms for implementation.

Legal frameworks governing AI

Many governments in the region highlight the need to evaluate current legal frameworks and to adopt new legislation. Unlike many areas of government policymaking, AI is a cross-cutting issue with potential impacts in many different policy areas or sectors, governed by different legal regimes. The countries of Europe and Central Asia are increasingly understanding that they need to keep pace with AI progress and manage the risks. As more governments apply AI in the delivery of their public services, there is also growing awareness of the need to address the impact of AI systems on people's lives. The development of national AI strategies can create a common framework for implementation in both the public and private sectors.

AI involves a number of different technologies (e.g. machine learning, image and speech recognition, natural language processing), with different levels of complexity and use, which may have a significant impact on a broad range of human rights. Countries are starting to develop sector-specific regulations for different fields of AI (e.g. self-driving vehicles). As advocated by the European Center for Not-for-Profit Law (ECNL), to achieve these safeguards CSOs must also be proactively involved in their creation.[55] Civil society involvement "brings expertise and real-life examples about the impact of AI-based systems on different groups of people, including risks to human rights".[56] This contributes to the rights-respecting use and deployment of AI and will support trust in the use of AI systems throughout societies.

Globally, some 50 countries have adopted national AI strategies. While AI regulation is nascent, many are beginning to elaborate national AI strategies and policies, addressing the economic, social and ethical implications of AI advancements. For the majority of governments in the region, where the use of AI in public services is still in its infancy, strengthening the capacity to effectively realize human rights builds an essential foundation for the responsible use of AI.

According to the 2020 edition of the Government Artificial Intelligence Readiness Index which covers 172 countries, Serbia scores highest (46) compared to all the other countries in the region. Next in the order is Ukraine (57), followed by a group of closely ranked countries: Kazakhstan (64), Azerbaijan (65), Belarus (66), Türkiye (67) and Georgia (72). Based on the index, Uzbekistan (95), Kyrgyzstan (102), Bosnia and Herzegovina (100) and Tajikistan (112) are significantly less prepared for the development of AI. While the focus of the index is on government readiness to implement AI in the delivery of public services, the indicators also show the degree of AI readiness of the private sector and society as a whole. It measures 33 indicators grouped across 11 dimensions, including vision, governance and ethics, data availability, data representativeness and human capital.[57]

55 ECNL, "Country papers on participatory processes in drafting national AI policies in the Czech Republic, the Netherlands, Australia and Canada", 19 April 2021, available at https://ecnl.org/publications/being-ai-ware-incorporating-civil-society-national-strategies-artificial-intelligence.

56 Ibid.

57 Oxford Insights and the International Development Research Centre, "AI Readiness Index 2020", available at https://www.oxfordinsights.com/government-ai-readiness-index-2020.

Serbia, Türkiye and Ukraine have already published national AI strategies. Bosnia and Herzegovina plans to prepare one. Azerbaijan is in the process of developing its AI strategy and Tajikistan has a draft strategy in consultation. North Macedonia intends to develop one soon and has created a Working Group for this purpose. Kazakhstan previously had a Roadmap for AI and other smart technologies. As part of its 2030 Digital Uzbekistan programme, Uzbekistan launched a strategy for the development of AI and an appropriate legal framework. The practical and effective implementation of these strategies will be key.

The public sector has two major roles to play in the development of AI and therefore faces a dual challenge. Firstly, the public sector should promote the formation of a national ecosystem for start-ups and industry aimed at the utilization of AI, using AI applications in different sectors, and achieving socio-economic growth, well-being and prosperity. Simultaneously, the government should create a regulatory framework that balances and reduces the threats, risks and challenges associated with AI systems and that provides effective mechanisms for enforcing the adopted legal, human rights and ethical standards.

Many of those interviewed for the scoping study lamented the lack of a people-centred digital transformation in countries across the region. In many cases, the primary focus of State efforts is perceived to be safety, security and efficient digitalization of State services, rather than openness, transparency and a clear response to citizens' needs. There is a need to have a balanced discussion, including meaningful public participation. As countries in the region start to have ethical, moral and philosophical debates on AI, it is important that the relevant issues related to the use of AI in both the public and private sectors are discussed in all their complexity and in light of applicable human rights standards.

Central Asia

The countries in Central Asia have adopted comprehensive data protection and privacy laws, with Uzbekistan's being the most recent (enacted in 2021), together with the amendment of the law in Kazakhstan adopted in 2021 to address data localization and introduce better enforcement mechanisms. However, none of them have yet been found adequate by the EU. The Enhanced Partnership and Cooperation Agreements with the EU provide a framework for the EU's bilateral relations with Central Asian countries. Together with the adoption of the new EU Strategy on Central Asia in May 2019, they provide an opportunity to enhance cooperation on data protection and cybersecurity.[58]

Along with ambitious national strategies for digitalization and innovative development, the countries of Central Asia are actively developing services in biometrics, artificial intelligence, video surveillance systems and facial recognition. This reinforces the importance and the need to build a culture of protecting personal data in the region.

58 European Commission, The EU and Central Asia: New Opportunities for a Stronger Partnership, JOIN(2019) 9 final, 15 May 2019, p. 6, available at https://eeas.europa.eu/sites/default/files/joint_communication_-_the_eu_and_central_asia_-_new_opportunities_for_a_stronger_partnership.pdf.

Raising awareness about data protection requirements should be one of the priority areas for digitalization in Central Asia.

South Caucasus and Eastern Europe

The countries of the South Caucasus and Eastern Europe region, including EU candidate States Ukraine and Moldova, are members of the EU's Eastern Partnership (EaP), which aims to strengthen political and economic relations between the EU, its Member States and partner countries, as well as supporting sustainable reform processes. This includes the improvement of legal regulation for data protection. Furthermore, the COE/EU Programme Partnership for Good Governance (PGG) provides tailored support to Eastern Partnership countries to bring legislation and practice closer to European standards in the fields of human rights, rule of law and democracy.[59] It supports the further development of rights-based legislative and regulatory frameworks on data protection, and effective implementation of data protection principles in the region. In terms of cybersecurity—which is also important for the protection of data and critical information systems, as well as for protection against the threat of cyberviolence—Azerbaijan, Georgia, Moldova and Ukraine have already put forward national strategies and action plans, while Armenia and Belarus currently lack comprehensive legal frameworks or state cybersecurity policies.[60]

The Western Balkans and Türkiye

Together with Türkiye, countries including Albania, Bosnia and Herzegovina, Montenegro, Serbia and North Macedonia are Member States of the Council of Europe, with the exception of Kosovo due to its status as a disputed territory.[61] In terms of the international legal framework, of primary importance to the provision of privacy and data protection safeguards in this subregion are the Council of Europe's treaties pertaining to fundamental freedoms such as the European Convention on Human Rights and the Budapest Convention (Convention on Cybercrime).

In addition, the EU Stabilisation and Association Agreements, as the main documents related to the enlargement process, foresee obligations for all the Western Balkan countries to align their national legislation with EU acquis, including the GDPR. Similarly, Türkiye is required to align its legislation as part of EU accession negotiations and cooperation facilities (e.g. Horizontal Facility for the Western Balkans and Türkiye 2019–2022). In such cases, the EU Digital Strategy should also be viewed as a basis for the introduction of data governance policies and reforms, and the forthcoming EU Global Digital Cooperation Strategy will also be of relevance to the countries in the region as they closely cooperate with EU countries and will be aligning their policies with the EU.

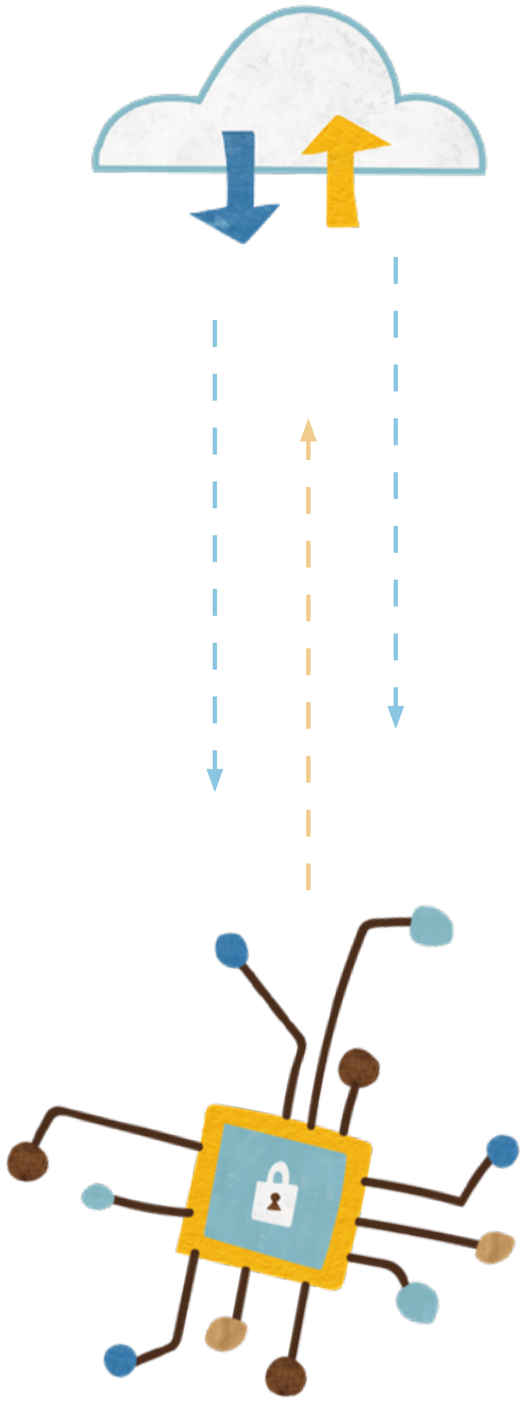
59 Council of Europe and European Union, "Partnership for Good Governance II", available at https://pjp-eu.coe.int/en/web/pgg2/home.

60 For cybersecurity governance assessments of these countries, see DCAF, "Programmes: Cybersecurity Governance", available at https://www.dcaf.ch/cybersecurity-governance.

61 As elsewhere in this report, references to Kosovo shall be understood to be in the context of Security Council Resolution 1244 (1999).

Regarding national cybersecurity frameworks, the Western Balkan countries and Türkiye recognize the need for adopting a comprehensive approach. Albania has a Law on Cybersecurity and Kosovo has adopted a National Cybersecurity Strategy with a complementary action plan, although it has yet to adopt a specific law regulating this field. Montenegro has already adopted its second National Cybersecurity Strategy and also has an Information Security Law. North Macedonia has a National Cybersecurity Strategy and Action Plan, while both Bosnia and Herzegovina and Serbia each have a Law on Information Security, although not yet an official cybersecurity framework.[62] In Türkiye, the relevant legislation is still evolving, and cybersecurity rules are not consolidated under one legislative instrument but rather under different sector-specific regulations.

Without prejudice to its current status, the Council of Europe has been supporting Kosovo through cooperation activities since 1999, in full compliance with UN Security Council Resolution 1244.[63] These activities include assistance in bringing legislation, institutions and practice further into line with Council of Europe standards, including those in the area of data protection and privacy rights. The document providing an overview of cooperation activities and the EU/Council of Europe Joint Programme Horizontal Facility for the Western Balkans and Türkiye provide a framework for this cooperation and make explicit reference to privacy and data protection.[64]



62 Irina Rizmal, Legal and policy frameworks in Western Balkan economies on PPPs in cybersecurity (DCAF, 2021), available at https://www.dcaf.ch/sites/default/files/imce/ECA/LegalPolicyFrameworksCS_PPPs_WB_mar2021.pdf.

63 See COE, "Kosovo*", available at https://www.coe.int/en/web/programmes/kosovo.

64 Council of Europe, Committee of Ministers, "Overview of Co-operation Activities in Kosovo*", 16 November 2021, GR-DEM(2021)11, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680a48e48.

3 Digital transformation and governance of AI

AI and digitalization serve as strategic enablers for public administration reform, good governance and evidence-based policies, as well as to ensure interoperability, trust and openness. Advanced digital and e-government services can also be a tool for empowering citizens to contribute to decision-making in diverse communities. Furthermore, digitalization functions as an enabler for achievement of the Sustainable Development Goals (SDGs), in the framework of the core principle of leaving no one behind. During the pandemic, the need for strengthened support and investments in digitalization efforts and effective digital governance across the region was highlighted, specifically for achieving continuity and delivery of core government functions and services.

The deployment of AI within the public sector raises particular risks for human rights, given the high-impact nature of policies and decisions, the potential of increased discrimination, heightened privacy issues and other legal challenges. Given that it may be impossible for an individual to opt out of public services, at least without facing negative consequences, precautions and safeguards are needed for the use of AI and automatic decision-making systems in public governance and administration. Within Europe and Central Asia, it would be useful to establish a common framework to evaluate the potential impact on human rights of the use of AI and automatic decision-making systems in the public sector. According to the ruling of a landmark case in the Netherlands, governments have a "special responsibility" to safeguard human rights when implementing AI and automated decision-making systems.[65]

65 Adamantia Rachovitsa and Niclas Johann, The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case, Human Rights Law Review, Volume 22, Issue 2, June 2022, available at https://doi.org/10.1093/hrlr/ngac010.

Overview of international AI regulation frameworks

To facilitate the development of ethical guidelines for AI, many governments around the world have established AI ethics committees and councils. Some governments also implement monitoring and reward systems for compliance with principles for trustworthy AI. Within the EU, various Member States have set up AI observatories and knowledge centres to support and enable socially responsible and ethically sound implementation of AI. Numerous guidelines by technical experts, sector representatives, national bodies and others also promote the responsible development and use of trustworthy and ethical AI.

Within the EU, a number of important data and AI legislative initiatives have been proposed, including the "European Commission Proposal for a Regulatory Framework on Artificial Intelligence" (the EU AI Act).[66] The proposed EU AI Act is currently being negotiated and adopts a risk-based approach to AI, where regulation is proportional to the "impact" of AI systems on people's lives. Other relevant initiatives at the EU level include the "Digital Services Package" and the "European Data Strategy 2020". In 2019, the OECD released a "Recommendation on Artificial Intelligence", which includes a set of principles for responsible stewardship of trustworthy AI. The OECD also provides the Secretariat for the Global Partnership on AI (GPAI) launched in July 2020, an international initiative to spur the responsible development and use of AI with full respect of human rights, inclusion, diversity, innovation and economic growth.

At the Council of Europe level, an "Ad Hoc Committee on Artificial Intelligence" (CAHAI) has been established to examine the feasibility and potential elements of a legal framework for the development, design and application of AI systems compatible with human rights, democracy and the rule of law. Recognizing the limitations of voluntary ethics guidelines, the CAHAI explicitly aims to ensure the protection of human rights, democracy and the rule of law through a mix of legally binding and non-binding instruments. This work involves all sectors of the Council of Europe as well as specialized instruments such as the Ethical Charter on the Use of AI in Judicial Systems that was prepared by the Commission for the Efficiency of Justice (CEPEJ).[67] As part of its work, CAHAI conducted

66 European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, 21 April 2021, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

67 Council of Europe and European Commission for the Efficiency of Justice, European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, December 2018,

a multi-stakeholder consultation process; the findings revealed that stakeholders want assurance that AI systems will be assessed based on a human rights and freedoms framework.[68]

At the UN level, the UNESCO Social and Human Sciences Commission has approved a "Recommendation on the Ethics of Artificial Intelligence" which is the first ever global standard-setting instrument on the ethics of AI, relevant to all 193 UNESCO Member States.[69] UNICEF has developed draft "AI Policy Guidance for Children", which includes "Recommendations for building AI policies and systems that uphold children's rights to meaningfully include children in AI development, to protect children's data and privacy, while prioritizing fairness in AI systems that affect them and to ensure children's safety in an AI world".[70] In 2019, the "UN Global Pulse Expert Group on Governance of Data and AI" (formerly the Data Privacy Advisory Group) expanded to incorporate greater expertise in AI ethics and human rights.[71] Members' expertise informs the development of strategies and guidelines on the ethical and privacy-protective use of data and AI for purposes of sustainable development, humanitarian action and peace.

"The Boston Global Forum" (BGF) and "Nizami Ganjavi International Center" (NGIC) in Azerbaijan have announced a collaboration to promote initiatives related to a Global Alliance for Digital Governance. The initiative also involves the "UN Centennial Initiative, AI World Society" (AIWS) and "the Club de Madrid". Under the agreement, the NGIC will connect the governments of Balkan and Middle East nations to support the "Global Alliance for Digital Governance" (GADG), contributing to the creation of a Global Accord on AI and Digital Rights.[72]

NATO Defence Ministers adopted a strategy on AI in October 2021, setting out standards for its use according to international law (Albania, Montenegro, North Macedonia and Türkiye are all NATO members).[73]

Notable applications of the international human rights framework to issues of AI governance can be found in various resolutions of the UN Human Rights Council and in reports published by several UN Special Procedures.[74] A 2021 report by the UN High Commissioner for Human Rights, "The Right to Privacy in the Digital Age" which draws attention to the risk of discrimination linked to AI-based decisions, also acknowledges that States have a specific "duty to adopt adequate legislative and other measures to safeguard individuals against interference in their privacy, whether it emanates from State authorities or from natural or legal persons."[75] Similarly, the Human Rights Council has published a report on the implications of emerging technologies for human rights. Moreover, the UN OHCHR has recently called for a moratorium on facial recognition and other AI systems.

Overview of regional policies and frameworks for AI and digital transformation

As countries in the region start to have ethical, moral and philosophical debates on AI, "it is important that the issues are discussed in all their complexity, and infused with human rights concerns, with respect to using AI in both the public and private sectors".[76] The public sector has two major roles to play in the development of AI and therefore faces a dual challenge. Firstly, the public sector should promote the formation of a national ecosystem for start-ups and industry aimed at making the most of AI, using AI applications in different sectors, and achieving socio-economic growth, well-being and prosperity. Simultaneously, the government should create a regulatory framework that balances and reduces the threats, risks and challenges associated with AI systems and that provides effective mechanisms for enforcing the adopted legal, human rights and ethical standards.

According to the Government Artificial Intelligence Readiness Index 2021, which focuses on government readiness to implement AI in the delivery of public services, as well as readiness of the private sector and society as a whole, Serbia (56) and Türkiye (57) have the higher readiness compared other countries in the region.[77] While Ukraine (64), Kazakhstan (66) and Azerbaijan (67) are among countries with a stronger readiness, the study also reveals that Central Asia is one of the regions with countries that score lowest with Tajikistan (98) and Kyrgyzstan (100) being significantly less prepared for the development of AI compared to other countries in the region. The majority of the countries in the region are below the global average (47.41) for AI readiness.

The details on how human rights should be protected in the context of AI are largely missing in the majority of strategy documents. There is a need to provide deep analysis or assessment of the impact of AI applications on human rights. Countries in the region should engage CSOs for ensuring that safeguards for fundamental rights and freedoms are included in their AI strategies.

As advocated by the European Center for Not-for-Profit Law, to achieve these safeguards CSOs must be proactively involved in their creation to contribute their expertise and real-life examples about the impact of AI-based systems, including risks to human rights, on different groups of people.[78] This will also contribute to rights-respecting use and deployment of AI to ensure innovation does not come at the cost of human rights.

AI readiness of the countries in the region

Regional position	Global position	Country	Overall score	Government	Technology sector	Data and infrastructure
1	56	Serbia	55.98	68.15	36.35	63.42
2	57	Türkiye	55.49	71.41	39.05	55.99
3	64	Ukraine	50.58	52.36	38.19	61.19
4	66	Kazakhstan	48.43	48.80	32.38	64.10
5	67	Azerbaijan	48.26	50.60	33.86	60.34
6	73	Belarus	46.20	39.89	34.30	64.40
7	75	Montenegro	46.10	40.71	34.61	62.96
8	76	Armenia	45.93	43.10	31.14	63.53
9	79	Georgia	45.41	44.20	29.22	62.83
10	81	North Macedonia	43.73	40.79	31.08	59.31
11	83	Albania	42.90	41.47	28.54	58.69
12	86	Republic of Moldova	41.71	40.03	29.80	55.29
13	93	Uzbekistan	40.13	37.95	31.32	51.13
14	96	Bosnia and Herzegovina	38.67	31.05	27.10	57.87
15	98	Tajikistan	38.49	35.85	26.29	53.31
16	100	Kyrgyzstan	37.61	35.16	23.62	54.04

Source: Data are from the Government AI Readiness Index 2021

Central Asia

Central Asia is one of the regions that scores lowest in the Oxford Insights Government AI Readiness Index. The World Bank is financing a 'Digital CASA' project in Central Asia and parts of South Asia, through which regionally integrated digital infrastructure is to be developed and an enabling environment supported, aimed at increasing access to more affordable Internet, expanding private investment in the ICT sector, and improving government capacity to deliver digitally public services. In February 2021, UNESCO hosted a round table on the development of AI in the region, with experts from civil society, private sector and governments attending to facilitate dialogue on the multiple implications of AI in line with UNESCO's Internet Universality ROAM Principles (Rights, Openness, Access and Multi-stakeholder participation).[79] This followed the launch of the report, Steering AI and Advanced ICTs for Knowledge Societies: A ROAM Perspective, translated into Russian. The report covers how AI and advanced ICTs will impact human rights, openness and access, and how a multi-stakeholder approach can steer the development and usage of AI in ways that mitigate risks and achieve the Sustainable Development Goals.[80] UNESCO is also cooperating with UNITAR on delivery of a micro-learning course on AI and human rights for youth aged 16 to 24 (not specific to the region). The course focuses on how freedom of expression, right to privacy and the right to equality are impacted by AI.[81]

South Caucasus and Eastern Europe

The EU intends to extend the Digital Single Market to the Eastern Partnership and the European Action Plan for Human Rights and Democracy (2020–2024) and recognizes new technologies as one of the key priority areas for external human rights policy.[82] This includes the improvement of legal regulation for data protection. Furthermore, the COE/EU Programme Partnership for Good Governance (PGG) provides tailored support to Eastern Partnership countries to bring legislation and practice closer to European standards in the fields of human rights, rule of law and democracy. It supports the further development of rights-based legislative and regulatory frameworks on data protection, and the effective

available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

68 ECNL, Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI): Public consultation (survey) March 30–April 29, 2021 – ECNL Answering Guide, available at https://ecnl.org/sites/default/files/2021-04/CAHAI%20Survey_ECNL%20Answer%20Guide_0.pdf.

69 UNESCO, "Recommendation on the ethics of artificial intelligence", available at https://en.unesco.org/artificial-intelligence/ethics.

70 UNICEF, Policy guidance on AI for children 2.0, November 2021, available at https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children.

71 UN Global Pulse, "Expert Group on Governance of Data and AI", available at https://www.unglobalpulse.org/policy/expert-group-on-governance-of-data-and-ai/.

72 EU Reporter, "Distinguished leaders from Boston and Balkan regions to collaborate for Global Law on AI and Digital Rights", 1 October 2021, available at https://www.eureporter.co/world/us/2021/10/01/distinguished-leaders-from-boston-and-balkan-regions-to-collaborate-for-global-law-on-ai-and-digital-rights/.

73 Agnes Szucs, "NATO defense ministers adopt strategy on artificial intelligence", Anadolu Agency, 22 October 2021, available at https://www.aa.com.tr/en/world/nato-defense-ministers-adopt-strategy-on-artificial-intelligence/2400087.

74 For example, the "Report on Artificial Intelligence technologies and implications for freedom of expression and the information environment", A/73/348; the "Report on the use of digital technologies in the welfare state", A/74/493; the "Report on the rights to freedom of peaceful assembly and of association: The Digital Age", A/HRC/41/41; and the "Report on racial discrimination and emerging digital technologies: a human rights analysis", A/HRC/44/57.

75 UN High Commissioner for Human Rights, Report on the Right to Privacy in the Digital Age, A/HRC/48/31, 13 September 2021.

76 Michael Pizzi, Mila Romanoff and Tim Engelhardt. "AI for humanitarian action: Human rights and ethics". IRRC No. 913. March 2021. https://international-review.icrc.org/articles/ai-humanitarian-action-human-rights-ethics-913.

77 Oxford Insights and the International Development Research Centre, "AI Readiness Index 2021", available at https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/61ead0752e7529590e98d35f/1642778757117/Government_AI_Readiness_21.pdf.

78 ECNL, "Country papers on participatory processes in drafting national AI policies in the Czech Republic, the Netherlands, Australia and Canada", 19 April 2021, available at https://ecnl.org/publications/being-ai-ware-incorporating-civil-society-national-strategies-artificial-intelligence.

79 UNESCO, "Experts from Central Asia debate the development of artificial intelligence in the region", 18 March 2021, available at https://en.unesco.org/news/experts-central-asia-debate-development-artificial-intelligence-region.

80 UNESCO, "Steering AI and Advanced ICTs for Knowledge Societies: A ROAM Perspective", 2019 (Russian translation in 2021).

81 UNESCO, 'Join UNESCO and UNITAR's AI and Human Rights course!", 27 September 2021, available at https://en.unesco.org/news/join-unesco-and-unitars-ai-and-human-rights-course; UNESCO, "Defending Human Rights in the Age of Artificial Intelligence", mobile micro-learning course, available at https://www.edapp.com/course/defending-human-rights-in-the-age-of-artificial-intelligence-2.

82 European Commission, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL – EU Action Plan on Human Rights and Democracy 2020–2024, 25 March 2020, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0005.

implementation of data protection principles in the region. In terms of cybersecurity, Azerbaijan, Georgia, Moldova and Ukraine have already put forward national strategies and action plans in this area, while Armenia and Belarus currently lack comprehensive legal frameworks or state cybersecurity policies.

The Western Balkans and Türkiye

Digital transformation is still lagging in many aspects in the countries of the Western Balkans. Efforts in bringing broadband Internet to all citizens of the Western Balkans region are well recognized; however, countries are less advanced in updating their strategic and regulatory documents. According to baseline research of the state of e-government development and digital literacy in selected Western Balkan countries for 2020, these countries are late with the harmonization of legal acts but are even more behind with the implementation of innovations.[83]

There is a Regional School of Public Administration (ReSPA) in the Western Balkans, established in 2010 as a joint initiative financed by the European Commission and World Bank. It places special emphasis on e-governance and runs a "Seasonal School on Digital Transformation".[84] However, the research found that public administrations in the region not only lack legislative but also technical capacities. Digitalization of public services in the Western Balkans region appears mostly driven by financial concerns, and many of the electronic services provided are intended for the business sector. Governments should define criteria for introducing e-government services based on citizens' needs. Moreover, citizens must be equipped with basic digital skills to help them understand how to avoid potential risks.

For countries in the region aspiring to join the EU, "improving the conditions for implementing digitalization, an initiative brought by the European Union in 2018, has been a chance to tackle various structural challenges while increasing transparency, openness and cross-regional cooperation".[85] However, since then, many of the countries in the subregion are experiencing political instability. Along with the pandemic crisis, it is feared that progress in implementation will be slowed down. Building on the EU's Digital Agenda for Europe 2010–2020, the EU's 2020 Economic and Investment Plan for the Western Balkans includes actions to prioritize and mainstream digitalization in national policies.[86] This plan offers an opportunity to accelerate the digitalization of governments, public services and businesses, in a manner consistent with the EU's values and legal framework. It advocates that the Western Balkans should use the EU's digital strategy as the guiding principle for a human-centric digital transformation of their economies and societies.[87] In line with EU efforts and guidelines, it aims to boost innovative digital transformation through encouraging the deployment of platforms and policies such as e-government, e-health, e-commerce, digital skills and virtual learning, open access to research data, investments into broadband and high-performance computing. It will foster the development of regional Digital Innovation Hubs supporting companies to boost their competitiveness using digital technologies, especially AI. And it will aim to enhance cybersecurity capacity and ensure the ethical use of technologies, including AI, in line with the EU Charter of Fundamental Rights and given a dynamic alignment with future EU legislation in this area. It will implement the Declaration on eGovernment, endorsed in Belgrade in 2019, to further accelerate work in line with the EU eGovernment action plan, in support of public administration reform.

83 MJAFT, "Digital Agenda Observatory – Baseline research of the state of e-government development & digital literacy in the targeted Western Balkan countries 2020", available at https://www.mjaft.org/en/reports/digital-agenda%E2%80%AFobservatory%E2%80%AF-baseline-research-state-e-government-development-digital.

84 ReSPA, "Seasonal School on Digital Transformation – Using Emerging ICT Technologies in Public Administration", 25 October 2021, available at https://respaweb.eu/0/news/422/seasonal-school-on-digital-transformation--using-emerging-ict-technologies-in-public-administration.

85 European Commission, An Economic and Investment Plan for the Western Balkans, COM(2020) 641 final, 6 October 2020, available at https://ec.europa.eu/neighbourhood-enlargement/system/files/2020-10/communication_on_wb_economic_and_investment_plan_october_2020_en.pdf.

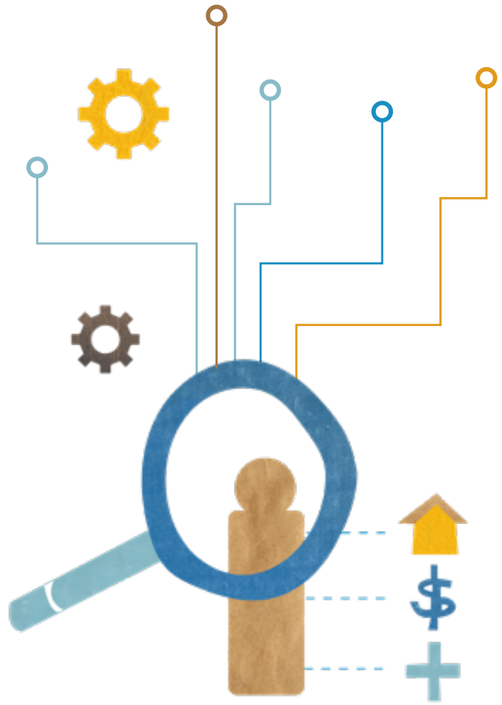
86 European Commission, Measures in support of a Digital Agenda for the Western Balkans, SWD(2018) 360 final, 22 June 2018, available at https://www.rcc.int/download/docs/Measures%20in%20Support%20of%20a%20DA%20for%20the%20WB.pdf/aa23a16b69061b98e4d0eb62390e751a.pdf.

87 European Commission, Communication on Shaping Europe's digital future COM/2020/67 final, 19 February 2020, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52020DC0067.

4 Specific sectors at higher risk of human rights impacts: a human rights–based approach

While the use of technology and AI can lead to bettering the lives of people, it can, at the same time, be a threat to human rights in certain sectors. Globally, there has been pressure to establish clearer guidelines for the development and use of AI technologies in areas that may present particular risks to human rights. According to the UN's "The Right to Privacy in the Digital Age" report, law enforcement, national security, criminal justice, and border management as well as public services, employment, and content moderation have a higher risk to privacy and associated rights than others.[88] This is especially true if there are no set safeguards and mechanisms to protect the use and processing of data by companies and governments. As EC's White Paper on Artificial Intelligence states "the main risks related to the use of AI concern the application of rules designed to protect fundamental rights."[89] Deploying AI systems in public service areas requires particular attention from an ethical and human rights perspective. The CoE CAHAI has underlined the fact that any AI system used in the public sector will give rise to certain issues related to human rights, democracy and the rule of law and it is therefore important to give due consideration to the use of AI systems in this field.[90]

Risks to human rights may occur especially when AI systems are used to make high-impact or legally consequential automated decisions, which are likely to exert a disproportionate impact on people in situations of vulnerability and may lead to distributive injustice. The automatic processing of data about a person's health, job, welfare or credit can lead to decisions with discriminatory or unfair results. For example, in 2015, Amazon's hiring algorithm was found to be biased against women "because the algorithm was based on the number of resumes submitted over the past ten years, and since most of the applicants were men, it was trained to favour men over women".[91] In such cases, a comprehensive risk assessment framework, transparency about the goals and when the algorithms are used, and robust accountability mechanisms are essential to accurately assess actual positive and negative impacts. The use of AI in financial services has also been highlighted as a potential area of risk from a human rights and anti-discrimination perspective especially for the groups that have been historically underrepresented.[92] The Centre for Data Ethics and Innovation issued a report about bias and algorithmic decisions and stated that financial entities mostly count on concrete and detailed prognoses about how people would behave in, for instance, debt repayment.[93] The report also indicates that some disadvantaged groups are prone to historic biases in the algorithmic systems and there is a high chance of being discriminated against, therefore, "data quality, inclusion, and transparency" are essential.[94] Within the EU context, there has been much discussion about red lines for AI systems that pose unacceptable levels of risk. One commentator proposes that governments should collaborate to establish a set of global "Red Lines" to prohibit the development and use of AI in specific applications that might pose an ethical or existential threat to humanity and the planet.[95] It is suggested that they create a set of "Green Zones" for scientific diplomacy and cooperation in order to capitalize on the opportunities that AI may represent in confronting major collective challenges such as crises in health, climate and energy, and achieving the Sustainable Development Goals.



88 OHCHR, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/48/31, 13 September 2021, available at https://undocs.org/A/HRC/48/31.

89 European Commission, White Paper on Artificial Intelligence – a European Approach to Excellence and Trust, COM(2020) 65 final, 19 February 2020, p. 11, available at https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

90 Council of Europe CAHAI-PDG, Report of 6th online meeting (11 to 12 October 2021), para. 4 (15), available at https://rm.coe.int/cahai-pdg-2021-pv4-meeting-report-6th-meeting/1680a45412.

91 Terence Shin, "Real-life examples of Discrimination Artificial Intelligence", 4 June 2020, available at https://towardsdatascience.com/real-life-examples-of-discriminating-artificial-intelligence-cae395a90070.

92 Centre for Data Ethics and Innovation (2020), Review into bias in algorithmic decision-making, November 2020, pp. 48–61, available at https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making.

93 Centre for Data Ethics and Innovation, "Review into bias in algorithmic decision-making", November 2020, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf.

94 Ibid., p. 7.

95 Francesco Lapenta, Our Common AI Future: A Geopolitical Analysis and Road Map for AI Driven Sustainable Development Science and Data Diplomacy (2021), available at https://dataethics.eu/our-common-ai-future/.

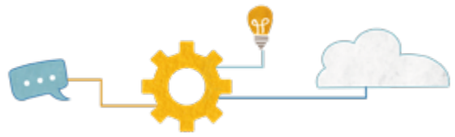
Risk management, transparency, documentation and data quality have emerged as methods for both technology companies and States to identify, mitigate and remedy the potential risks and harms of AI and algorithmic systems. EU's proposal AI Act (AIA) sets out a risk-based approach to AI regulation and highlights the importance of respecting the precautionary principle where the potential negative impact is higher than the benefits. According to the Act, high-risk AI systems shall comply with a set of specific requirements, established by the AIA. A risk management system shall therefore be established, implemented, documented and maintained in relation to such high-risk AI systems. Human Rights Risk Assessments (HRRAs) and Human Rights Impact Assessments (HRIAs) are also being discussed as an important tool, drawing on work previously carried out on Algorithmic Impact Assessments or AIAs.[96] Existing standardization work will also be relevant in this context.[97]

With the European Commission's Proposal for a Regulation laying down harmonized rules on AI, the EU has the opportunity and the responsibility to assess the impact of AI on the full spectrum of fundamental rights. EU law already requires Impact Assessments in specific sectors, such as Data Protection Impact Assessments (DPIAs) under the GDPR (Article 35). It would therefore be useful to explore what can be learned from them for other fields and types of impact assessments.[98] The EU Assessment List for Trustworthy AI (ALTAI) specifically refers to the need to perform a fundamental rights impact assessment for AI systems and provides examples of relevant questions for this purpose.[99]

The Council of Europe also recommends that States should conduct human rights impact assessments in the area of AI before it is implemented. In particular, it is important for the public sector to conduct human rights impact assessments for their intended uses of AI and to ensure transparency and accountability. The CAHAI is currently developing a methodology to conduct Human Rights, Rule of Law and Democracy Impact Assessments for AI.[100] CAHAI is also developing guidance on the use of AI in the public sector. Also of relevance, its Working Group on Legal Frameworks (LDG) is exploring which sectors will require greater specific details and attention in terms of regulation by a possible legal instrument, e.g. the use of AI in law enforcement, judiciary and public administration. Furthermore, the Office of the United Nations High Commissioner for Human Rights (OHCHR) is developing UN system-wide guidance on human rights due diligence and human rights impact assessments in the use of new technologies, including through engagement with civil society, external experts and those most vulnerable and affected.

When considering the sectors exposed to human rights risk from the use of AI, it is important to ask questions such as:

- What uses of automated decision-making have the most impact on people?
- What data are used to make these decisions?
- What is the logic of the decision-making?
- If personal data are used, what are the stated processing purposes?
- What are the consequences of the decisions?
- What are the potential unintended consequences?



From a critical angle, one thing to consider when conducting a Human Rights Risk Assessment is whether a risk minimization approach is appropriate from the perspective of human rights. Several CSOs have advocated for the European Commission to adopt a rights-based, rather than a risk-based approach to AI regulation. It may therefore be useful to link HRIAs or HRRAs on AI to the UN Guiding Principles on Business and Human Rights as part of a due diligence framework. The digital HRIA of the Danish Institute on Human Rights could be a useful reference. It is also important to ensure a full AI life-cycle approach to the risk assessment process. Furthermore, a meaningful, timely and transparent multi-stakeholder participation should be ensured in HRIAs and HRRAs, as well as effective remedial mechanisms to redress any negative human rights impacts.

It is important to involve and support the role of civil society and affected communities in providing input into HRIA and HRRA pilot initiatives. Media and civil society activists have already established themselves as a driving force for accountability in AI and automated decision-making systems within Europe and the United States.[101]

96 For example, see Adriano Koshiyama and Zeynep Engin. "Algorithmic impact assessment: Fairness, robustness and explainability in automated decision-making." Presentation (Open Access) 6, no. 08 (2019).

97 The European Commission Joint Research Centre has conducted a high-level mapping of the significant AI standards onto the AIA requirements across areas such as data governance, transparency and human oversight; see S. Nativi and S. De Nigris, AI Watch: AI Standardisation Landscape, European Commission, 2021, available at https://www.standict.eu/sites/default/files/2021-07/jrc125952_ai_watch_task_9_standardization_activity_mapping_v5.1%281%29.pdf.

98 See Council of Europe, Artificial Intelligence and Data Protection: Challenges and Possible Remedies. Report on Artificial Intelligence, 27 January 2019, available at https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6; NIST, "Nist Risk Management Framework", available at https://csrc.nist.gov/Projects/risk-management; Swee Leng Harris, "Data Protection Impact Assessments as rule of law governance mechanisms", Cambridge University Press, 30 March 2020, available at https://www.cambridge.org/core/journals/data-and-policy/article/data-protection-impact-assessments-as-rule-of-law-governance-mechanisms/3968B2FBFE796AA4DB0F886D0DBC165D#.XoL9tjyutqQ.twitter.

99 European Union, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 17 July 2020, available at https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

100 A draft text has been approved by the CAHAI Policy and Development Group and was finalized at the final plenary meeting of CAHAI in May, 2021. The CAHAI fulfilled its mandate (2019-2021) and has been succeeded by the Committee on Artificial Intelligence (CAI).

101 For example, AlgorithmWatch at https://algorithmwatch.org/en/ and see Amnesty International, "Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal", 25 October 2021, available at https://www.amnesty.org/en/documents/eur35/4686/2021/en/.

5 Conclusions and recommendations for the adoption and governance of digital technologies and AI based on human rights

The overall sustainable and effective implementation of human rights in the context of digital transformation and during the rapid integration of new technologies requires the combined efforts and responsible approaches of a multi-stakeholder group of individuals, business enterprises, civil society, research, technical and academic communities, States and international organizations. Key components include political will, a strong legal framework, the presence of relevant institutions, a robust democratic (and accountability) framework, and a well-developed digital infrastructure and technical environment. Meaningful public participation and engagement is crucial to ensuring fair, just and equal digital futures. It is critical that civil society is a driving force and not just an observer of policy and regulatory developments concerning digital technologies and AI.

As the development arm of the United Nations, UNDP is in a strong position to support the inclusion of human rights in digitalization and digital transformation processes in Europe and Central Asia, based on both its technical expertise and strategic capacity-building, as well as on its trusted relationships with national, regional and local governments, civil society, the private sector, international organizations and development partners. UNDP is also well placed to serve as a knowledge hub for the region to provide research and advocacy on issues associated with the impact of digital technologies on human rights. Furthermore, a human rights–based approach is important to the implementation of UNDP's Digital Strategy 2022–2025.[102]

A set of recommendations is proposed below to ensure that the development, use and governance of digital technologies and AI in Europe and Central Asia is both people-centred and consistent with international human rights obligations. The recommendations are grouped according to both thematic area and stakeholder, with suggestions for strategic entry points and opportunities for UNDP support. While taking into consideration that the countries and territories of Europe and Central Asia may be at varying stages of technological advancement, the recommendations are designed to promote a human rights–based approach to legislation and policies for digital technologies and AI, including effective due diligence and accountability mechanisms; awareness-raising, training and capacity-building; and participation by diverse stakeholders.

Human rights in the governance of, and by, digital technologies and AI

Given that many countries in Europe and Central Asia are still in the early stages of adopting advanced digital technologies and AI, there is a critical opportunity to ensure an inclusive digital transformation that benefits all and respects human rights. As digital technologies become more embedded in society, in the economy and in the public sector, appropriate institutional, policy and regulatory frameworks, based on human rights, are needed. In particular, the use of automated and algorithmic decision-making systems within the public sector could pose significant risks for human rights if adequate governance arrangements are not in place and there is no meaningful participation of civil society and affected communities in the design, assessment, implementation and monitoring of digital initiatives.

UNDP should:

- Provide advice and support to States in the region to align regulatory, legislative and institutional frameworks for digital technologies and AI with human rights obligations and standards. This could include technical guidance on international normative standards and assistance in adopting them, as well as the development and dissemination of model frameworks and policies, and the provision of a regional forum for exchange of knowledge, best practice and peer learning.
- Conduct training and capacity-building on human rights and digital technologies for public officials, including law enforcement and judicial authorities, Parliamentarians, Data Protection Authorities and other relevant regulatory and enforcement bodies.

States should:

- Ensure that public sector bodies act consistently with human rights principles when procuring, developing or deploying AI systems or applications.
- Align regulatory, legislative, policy and institutional frameworks for digital technologies and AI with international human rights obligations; and engage with international AI governance initiatives, ensuring all efforts to elaborate guidelines or codes on the ethical implications of AI systems are grounded in human rights principles.

102 UNDP. Digital Strategy 2022–2025. Available at https://digitalstrategy.undp.org.

- Amend and/or enact privacy and data protection laws, policies and regulations, ensuring their effective implementation and recognizing rights related to automated decision-making and profiling.

- Introduce and strengthen accountability mechanisms to facilitate access to justice and redress for violations of human rights resulting from the use of digital technologies and AI.

- Take steps to address the digital divide and support citizens and vulnerable groups to access and use digital public services.

Civil society, media and National Human Rights Institutions (NHRIs) should:

- Play an active role in monitoring and reporting on digital regulation and initiatives, holding States to account on their compliance with international human rights commitments, as well as engaging in advocacy, research and policymaking.

Human Rights Impact Assessment of digital technologies and AI

Based on discussions with States and business enterprises in the region, as well as the UNDP network of accelerator labs, the UNDP Regional Hub in Istanbul could aim to identify which countries or companies are planning to implement or are currently implementing AI solutions or other digital technologies in sectors potentially exposed to risk from a human rights perspective. It is recommended that UNDP focus on Human Rights Impacts Assessments (HRIAs) in some of these sectors. Innovative efforts mostly tend to accommodate traditionally strong sectors. Given that most countries in the region are still only in the very early stages of planning or piloting AI systems, it may be advisable to widen the scope of the HRIAs to consider the use of digital technologies and automated or algorithmic decision-making processes more broadly.

UNDP should:

- For the conduct of HRIA pilots, consider developing or validating its own AI risk and impact assessment methodology, based on international efforts (including that by OHCHR) and considering local contexts.

- Build connections with the Danish Institute for Human Rights and the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), which have developed methodologies for HRIAs. UNDP country offices in the region could serve as internal leaders for championing human rights–based approaches and HRIAs in national digital transformation efforts by enhancing their own capacity in this area. The UNDP Regional Hub could consider developing an internal office manual or set of guidelines.

- Collect and publish a selection of public sector AI case studies from the region, including an analysis from a human rights perspective, and a set of generalized or more specific learnings from the HRIA pilots could also be published in the form of case studies.

Methodologies for HRIAs are being developed and promoted as important tools for the governance of digital technologies and AI, covering the full range of human rights that may be impacted. As technological features, services and functionalities are constantly evolving, it is important that potential human rights impacts are assessed prior to their deployment, and on a continuous basis thereafter. Meaningful, timely and transparent multi-stakeholder participation in HRIAs should be ensured, as well as effective remedies.

UNDP should:

- Develop, pilot and promote methodologies for Human Rights Impact Assessments of digital technologies and AI within Europe and Central Asia, building on existing efforts, as well as collaborating with relevant universities and research institutes, and including the perspectives of different stakeholders.

States should:

- Consider HRIAs when deploying digital technologies and AI systems within the public sector, especially in high-risk domains. Particular attention should be directed to the disparate impact of such technologies on racial, ethnic and religious minorities; women and children; people with disabilities; political opposition and activists.

Business enterprises should:

- Carry out HRIAs during the design and deployment stages of AI systems.

Civil society, academia and NHRIs should:

- Conduct or support ongoing research on the societal and human rights impacts of digital technologies and AI to provide an analysis that can be used in HRIAs.

Challenges to human rights posed by the use of digital technologies in the COVID-19 response

During the ongoing management of the COVID-19 pandemic, technological tools developed by government agencies and corporate entities have been used by States to track infections, enforce quarantine measures, maintain social distancing rules and track the administration of vaccines. States have also attempted to control the spread of inaccurate health-related information online. While measures to protect public health during the pandemic are necessary, there are risks that they may be too broad or discriminatory. Robust safeguards should be implemented to ensure any such measures are not misused by States or companies to collect confidential private information for purposes not related to the public health crisis. As many essential activities have moved online, it is also important to address the digital divide and ensure robust data protection frameworks.

UNDP should:

- Develop guidance on policy and good practices on human rights, COVID-19 and digital technologies (possibly with other UN entities) and organize regional workshops on lessons learned and safeguards to protect human rights.

States should:

- Ensure a human rights–based approach to the use of data and digital technologies during ongoing pandemic management and introduce and enforce safeguards, transparency and accountability mechanisms, e.g.:

  - Pandemic health measures and systems for health-related data should adhere to established international data protection and privacy principles.

  - The right to access information, as well as freedom of opinion and expression, should be respected, and public health emergency powers should not be used to limit access to information or prevent criticism of government policies.

  - Any technological surveillance carried out in the context of managing the pandemic must be proportional, lawful and necessary, and civil society and communities at particular risk should be consulted on public health measures involving technological responses.

Civil society, media and NHRIs should:

- Monitor and raise awareness where human rights may be impacted by the use of digital technologies in the COVID-19 response (e.g. rights to privacy, health, work, education, freedom of opinion and expression, freedom of assembly and non-discrimination)

Business enterprises should:

- Ensure decisions to take down online 'disinformation' about COVID-19 are based on clear and publicly accessible criteria and subject to appeal.

Human rights in the development and use of digital technologies and AI by the private sector

Business enterprises that develop, manufacture or deploy digital technologies and AI should observe the UN Guiding Principles on Business and Human Rights (UNGPs) and the OECD Guidelines for Multinational Enterprises. This means they should avoid infringing on human rights, as well as identify, prevent, mitigate and account for any adverse impact on human rights that they cause, to which they contribute or to which they are directly linked. States also have an obligation to protect persons within their jurisdiction from undue interference with their human rights by third parties, including business enterprises active in the technology sector.

UNDP should:

- Exercise leverage with global technology companies with which they are partners in order to promote a human rights–based approach to their activities. UNDP could provide a platform for multi-stakeholder engagement with these companies on their human rights obligations and facilitate meetings between government officials, innovation communities and civil society.

- Promote a human rights–based approach to online content moderation by social media platforms (e.g. by co-hosting regional workshops with OHCHR B-Tech, companies and local human rights actors or affected communities).

States should:

- Ensure that private sector design, development and implementation of digital technologies and AI systems give full consideration to human rights, particularly data protection, as well as ensuring effective external accountability mechanisms.

Business enterprises should:

- Comply with the UNGPs and OECD Guidelines and prevent, mitigate and remedy any adverse human rights impacts directly linked to their business

operations, products or services in their capacity as actors that design, develop, deploy or sell digital technologies and AI systems.

- Make explicit where and how AI technologies and automated techniques are used in their platforms, services and applications.

- Put human rights principles at the heart of online content regulation policies by social media platforms and publish data on content removal, including transparency on government requests and the rationale for important content moderation decisions, as well as providing effective remedy in cases of potential violations.[103]

- Avoid facilitating Internet shutdowns and censorship, including through contesting the legality of government orders, preserving and providing evidence, and providing effective remedies for past disruptions.

Civil society should:

- Consider ways to encourage the reporting of online hate speech through awareness campaigns and training.

Stakeholder engagement, public awareness and civil society capacity-building on digital technologies and AI

Civil society actors, human rights organizations and media in Europe and Central Asia can play a crucial role in protecting human rights by contributing to policy and legislation, monitoring and reporting on violations, and raising public awareness. It is therefore essential to support and empower a critical mass of civil society actors who can engage with governments, with the private sector and with regional and global institutions about the impact of digital technologies and AI on human rights, especially concerning historically marginalized or underrepresented communities, who are often disproportionately affected by the risks and harms posed by digital and data-driven interventions.

In order for a society to make critical judgements about the benefits and risks of digital technologies and AI, it must be given the opportunity to acquire knowledge about these technologies and their implications. UNDP could develop awareness-raising campaigns and training programmes on digital literacy and security, as well as on human rights in the digital space. This could be done in partnership with international organizations and with States in the region (e.g. by leveraging UNDP's programmes in schools), as well as through a network of CSOs. In this respect, it is important to demystify digital technologies and draw on real-world examples and case studies in order to highlight how they can impact on individuals and their rights, and also to make use of novel approaches, e.g. storytelling and online educational games, as well as to support the contribution of new voices and perspectives.[104]

UNDP should:

- Promote an inclusive debate between State authorities, the private sector, civil society, human rights groups and local communities on the impact of digital technologies and AI on human rights.

- Consider creating a secure UNDP cloud service for civil society in the region as a 'safe space' to connect and share information or strategies.

- Engage in capacity-building of civil society and media on opportunities and challenges for human rights related to digitalization, and support training on digital security and digital activism (e.g. using open-source methods).

- Engage in educational programmes and information campaigns to improve digital literacy and the skills of the general public, including on human rights and digital technologies.

States should:

- Provide support for the participation of civil society and affected stakeholders in decisions on the design, development and deployment of digital technologies and AI within public services, and on the regulation of digital technologies in the private sector.

Civil society should:

- Develop a regional civil society network on human rights and digital technologies to build alliances and collaborate on common challenges, as well as to foster peer learning.

- Raise awareness on human rights and digital technologies in ways that resonate with local contexts and communities.

- Provide training at regional, subregional and national levels on monitoring and advocacy related to human rights and digital technologies, including on thematic topics such as online content regulation, protecting children's rights online and protecting human rights in the context of technological responses to COVID-19.

- Engage with the UN Special Procedures and Treaty bodies, as well as with regional human rights mechanisms, on issues concerning human rights and digital technologies.

NHRIs, equality bodies and ombudsman institutions should:

- Build internal capacity and knowledge on human rights and digital technologies, support research and engage in outreach.[105]

Cooperation by the international community on human rights and digital technologies

There is an opportunity to enhance cooperation by the international community in response to the human rights challenges posed by digital technologies and AI. International development partners and standard-setting organizations should exchange good practices and collaborate in ensuring digitalization and digital transformation are informed by human rights principles and approaches.

UNDP should:

- Coordinate across relevant UN agencies, bodies and related data communities to translate human rights standards and ethical principles for digital technologies and AI into practical tools for stakeholders in Europe and Central Asia and engage with other international and regional development partners or standard-setting organizations active on these issues, such as the EU, Council of Europe, OSCE, World Bank, USAID and bilateral donors.

International and bilateral donors should:

- Conduct due diligence to ensure that programmes, projects, partnerships and grants supporting the use of digital technologies and AI are aligned with human rights.

103 For guidance, see BSR, A Human Rights-Based Approach to Content Governance, March 2021, available at https://www.bsr.org/reports/A_Human_Rights-Based_Approach_to_Content_Governance.pdf.

104 The UNESCO/UNITAR EdApp course on AI and human rights is a positive example, breaking down complex concepts about AI into activities centred around daily technology interactions (the course is currently being translated into Russian). Another good example is the 'Elements of AI' online course developed by the Finnish Government, which includes a module on AI ethics.

105 For example, see ENNHRI and EQUINET work on the topic of AI and anti-discrimination.

Addendum to the report

The impact of digital technologies and artificial intelligence on human rights in Europe and Central Asia in 2022

Executive Summary

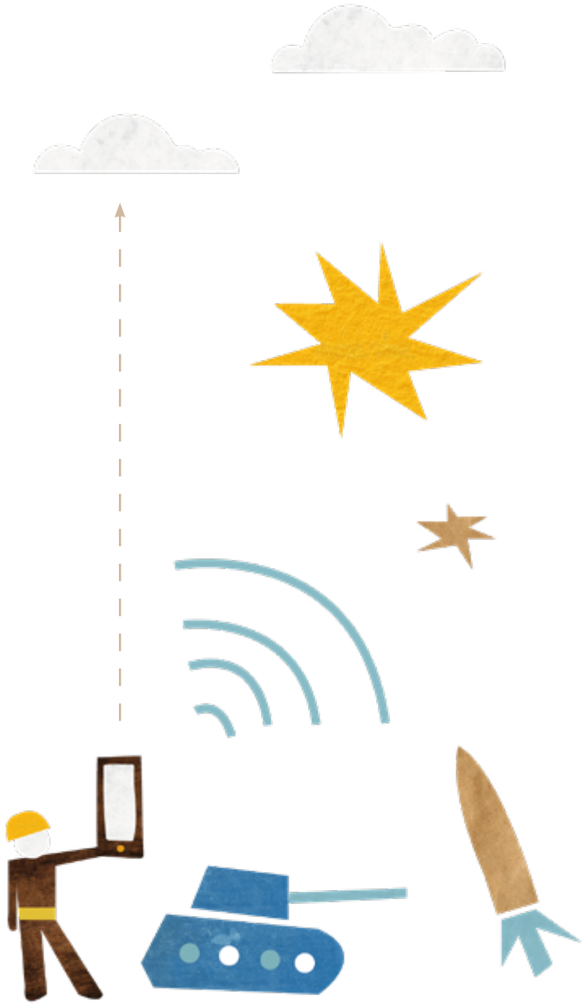
This addendum, 'The Impact of Digital Technologies and Artificial Intelligence on Human Rights in Europe and Central Asia in 2022', focuses on the trends, threats and developments around those technologies throughout the year 2022 with a special attention given to the impact of war and conflict on the varied uses of digital technologies and artificial intelligence, and vice versa.

The impact of the war in Ukraine is devastating, and has rapidly led to cascading political, humanitarian, economic and social crises. The war has caused one of the fastest forced population movements since World War II with around 7.8 million people forced to flee their homes.[106] The United Nations and its partners—which includes neighbouring and third countries—have scaled up operations, reaching 13 million people across Ukraine with life-saving aid.[107] Globally, the impact of the war on food security, energy and finance is systemic, severe and speeding up. We are on the brink of the most severe global cost-of-living crisis in a generation, affecting the lives and livelihoods of an estimated 1.6 billion people. In Ukraine alone, 17,362 civilian casualties have been reported as of 11 December 2022, including 6,755 killed, of which 424 were children, according to the OHCHR.[108]

The war in Ukraine has also illustrated the dual nature of digital technologies and artificial intelligence with adverse and damaging effects on human rights, for example, by advancing the use of drone attacks,[109] which are a contrast to the positive impacts of digital technologies on delivering aid and assistance. The use of digital technologies and artificial intelligence in Ukraine has enabled humanitarian actors to be more coordinated and efficient in their efforts to assist populations, while human rights violations were monitored not only by international and regional organizations with civil society, but also by civilians and citizens using similar digital technologies—mainly social media platforms, videos and photographs.

Significant and sustained efforts have been made to develop the global, regional and corporate governance of digital technologies and artificial intelligence over the last decade. It has included the adoption of international,[110] regional[111] and national[112] frameworks. Massive funding has been allocated to modernize governments and public services, to research and to innovation ecosystems. Global debates within the international community and regional blocs have created momentum for thinking about the risks and threats, ethical and societal implications of digital technologies and artificial intelligence. Today, there is a general consensus that innovation should generally be developed, implemented, monitored and regulated while using a human rights and risk-based approach to protect, support and uphold human rights law, international law and leaving no one behind.

This addendum[113] first highlights global and regional trends relating to digital technologies and artificial intelligence, highlighting patterns, practices and new threats, including cyberattacks, internet shutdowns, mass surveillance and facial recognition in public spaces. It then reviews evolutions of such trends at a country level with two distinctive lenses: on the one hand, digital technologies and artificial intelligence as drivers for innovation and change (e.g. e-government, e-public services and R&D) and on the other hand, digital technologies and artificial intelligence as a threat and/or source of human rights violations.



106 UNHCR. Operational Data Portal. Ukraine Refugee Situation, available at https://data.unhcr.org/en/situations/ukraine, accessed 15 November 2022.

107 UN News. "Ukraine: UN and partners provide life-saving aid to some 13.5 million", 10 November 2022.

108 OHCHR, "Ukraine: Civilian casualties as of 11 December 2022", 12 December 2022.

109 UN News. "Ukraine: Missile strikes, summary executions highlight importance of international law". 25 November 2022.

110 UNESCO Recommendation on the Ethics of Artificial Intelligence, the Berkeley Protocol, the Budapest Convention, A/HRC/49/L.31. etc.

111 EU GDPR, EU Artificial Intelligence Act, EU Digital Services Act, the European Media Freedom Act.

112 Laws, national strategies, codes of conduct, business policies, etc.

113 The addendum takes in consideration the developments in the region as of 15 September 2022.

General Trends

Global trends

2022 has confirmed that after COVID-19, digital technologies and artificial intelligence are important drivers for change and conflict, and highlighted this dual nature. Digital technologies and AI continued to improve the enjoyment and exercise of political, civil, economic and social rights (e.g. the freedom of expression, freedom of peaceful assembly, freedom of movement, and the rights to health and education) with the digitalization of public services (e.g. health, education, identity) and better access to internet services (e.g. e-government, e-media platforms, social media, e-banks), particularly in times of war and conflict.

The war in Ukraine also demonstrated that digital technologies and AI are playing an increased role during times of war and conflict for state and non-state actors for political, humanitarian and human rights purposes. They provide civil society (e.g. NGOs, human rights defenders, journalists, bloggers) with the means to defend and advocate for human rights and monitor human rights violations. They provide humanitarian actors with new means and tools to provide assistance and aid more rapidly and effectively to the populations in need. Humanitarians have heavily relied upon such technologies to provide digital humanitarian aid during the war in Ukraine. Technologies were deployed at borders to face an unprecedented migration crisis using cash-based services to enable internally displaced persons (IDP) to have access to necessity goods. Digital technologies and AI systems were also used to coordinate responses and communicate with staff, other agencies and neighbouring countries.

At the same time, the year 2022 confirmed the trends of harm caused by digital technologies and AI, that had already appeared before COVID-19 and continued during the pandemic. The trends increased in terms of geographic scope, reach, volume, intensity, speed and precision of targeting groups or specific individuals. The datafication of society and the interoperability of services across countries (e.g. citizen digital identities, digitalization of humanitarian aid) have facilitated and amplifies those trends, which could become exponentially detrimental to human rights, as reliance on digital services increases, trust in global and national governance is questioned and mistrust is amplified by targeted misinformation campaigns and by the lack of algorithmic transparency (also called the 'black box' effect).

The year 2022 also confirmed that digital technologies and AI continue to be the "Wild West for human rights",[114] characterized by the digital divide, data privacy breaches, extraction of sensitive data, disinformation campaigns, hate speech, microtargeting, biased algorithms, proliferation of spyware and other tools,[115] and cyberattacks. The United Nations Secretary-General called the internet a "5-alarm" fire,[116] that today threatens peace and security.

Among those threats, internet shutdowns have been frequently and systematically used worldwide during times of war and conflict and political unrest such as protests, political dissidents' movements and coups. The shutdowns include actions that limit the ability of a large number of people to use online communications tools, either by generally restricting internet connectivity or by obstructing the accessibility and usability of services that are necessary for interactive communications, such as social media and messaging services.[117] The latter action reflects the techniques used over the years 2021 and 2022: internet shutdowns by targeting telecommunication infrastructures or communication networks, blocking websites, cutting off the internet including mobile internet,[118] blocking IPs, blocking access to VPNs[119] or banning their use,[120] 'blocking of particular services or applications, such as social media platforms and messaging apps, the slowing down of internet traffic to impede connectivity'[121] ('throttling') and limiting mobile services to 2G.[122] Such practices hamper access to the internet and consequently render it extremely difficult to make a meaningful use of it to share or watch videos and/or photographs, to livestream events, to access information from multiple sources, to spread information and to connect with relatives. In countries where internet access is still limited in terms of infrastructure and/or affordability or where the population conversely mainly—if not exclusively—uses mobile connections, such practices amplify inequalities facing vulnerable groups. In some contexts, such practices 'may amount to a complete internet blackout for the majority of the population',[123] thus violating and impeding the exercise of human rights.

Digital technologies and AI have accelerated the dissemination of information on social media and the internet. Information encompasses journalistic information, disinformation, fake news, deep fakes, propaganda and hate speech. In that respect, the war in Ukraine and conflicts worldwide have illustrated the impact of troll armies established for political purposes and the impact of digital tactics in times of war and conflict. Digital tactics include (re)tweeting certain information to preface, position and influence a narrative and justify political actions and/or to create, spread and amplify hate speech.[124]

Subsequently, the role of social media platforms when managing online content during times of war and conflict has also been questioned, as well as the threat of algorithms, data ecosystems and the business models of non-state actors (tech companies and social media platforms). Artificial intelligence systems[125] (machine learning, natural languages processing, biometrics, facial recognition) rely on a large amount of data that they collect, categorize, analyse, weigh in, prioritize, merge, share and monetize. AI-assisted curated content on social media platforms follows the same cycle. Social media algorithms rank data deciding what to amplify or downgrade, mostly according to the level of engagement (views, comments, likes, retweets, shares, saves) and relevancy. This can be adapted to specific contexts, groups, ethnicities and individuals using their beliefs, opinions, preferences and habits. The more people use such platforms (e.g. interactions, accepting cookies), the more the profiling is accurate, the more it jeopardizes their right to privacy, the more it supports unwilling—and most of the time unknown—intrusions into their lives. The profiling creates echo chambers that reinforce polarization, radicalization, hate speech and disinformation. In times of war and conflict, this phenomenon creates and exacerbates tensions and human rights violations such as the targeting of individuals (political opponents, civilians, human rights advocates, journalists, bloggers) and unlawful breaches of the right to privacy. Additionally, it can subject civilians to a flow of images of killings, atrocities and human rights violations based on the decisions made by an algorithm, and therefore spread fear and create unnecessary trauma.

In June 2022, the United Nations Special Rapporteurs[126] jointly noted "the role and responsibility of the tech sector and concern over content moderation policies and practices … disinformation and hatred online [as] a tactic often used by oppressive governments to justify persecution of minorities and dissenting voice, online and off",[127] while the United Nations constantly reaffirmed that "the same rights that people have offline must also be protected online".[128] To mitigate the risks and respond to an open call of civil society, social media platforms have over the years already adopted content moderation and violence policies,[129] which are general, country-specific or conflict-specific, depending on the platform. Yet, due to the visible, concrete consequences of online content during the war in Ukraine, those policies were challenged as to their relevance and efficiency in times of war and conflict.

In April 2022,[130] "terrifying photos and videos … were shared across various media outlets and social networks document[ing] killings of civilians, traces of torture, pillaging of civilian property and possessions, and other war crimes flood[ing] Facebook, Twitter and Telegram … Using its internal policies, Instagram began blocking content referenced with several hashtags",[131]—sometimes popular hashtags like #StandWithUkraine. It led to losing the documentation of human rights violations from various open sources. At the same time, it reopened a broader conversation within the international community[132] on the challenges to freedom of expression and the applicability of international humanitarian law and international human rights law to non-state actors—including companies, social media platforms and journalists—in times of war and conflict.

During the war in Ukraine, States' responsibility to protect their civilians and abide by their international obligations have been questioned and scrutinized in relation to both digitalization and cyberattacks. On the one hand, States worldwide have largely invested in the digitalization of their government (e-government) and public services (e.g. biometrics e-ID, public transportation, justice system during investigations or trials with facial recognition techniques and predictive analytics). On the other hand, States have faced an increased number of cyberattacks—sometimes sponsored by other States—a form of hybrid warfare. Cyberattacks can be cyberthreats, cyber influences and proper cyberattacks on State infrastructure (e.g. energy, telecommunication, government services) and populations. For example, specific algorithms have been used to destabilize or influence elections, polarize tensions between communities and position false narratives and fake news, thus undermining trust in the government, creating political unrest and instability and escalating conflicts. Consequently, States have taken measures to protect the public order, public safety and national security. In 2022,[133] internet shutdowns and the adoption of new legislation have been frequently used for the above-mentioned motives. Similarly, States have issued various laws criminalizing the spreading of fake news or disinformation. In some cases, such laws do not define a clear criterion for the identification of fake news and disinformation as national security threats. They have not introduced judicial supervision or monitoring or reporting mechanisms either. Countries have also increased requirements for platforms to be able to operate, such as registration with public authorities, special representatives to the government and country offices.

While protecting public order, public safety and national security, States shall need to find the right balance and observe these actions with their international commitments on human rights. They must ensure that any restriction is necessary, proportionate and non-discriminatory.[134] In that respect, the Road map for digital cooperation of the United Nations Secretary-General stresses that "blanket internet shutdowns and generic blocking and filtering of services are considered by United Nations human rights mechanisms to be in violation of international human rights law".[135] The Report of the Special Rapporteur on the

114 UN News. "Human rights 'inescapable and powerful'". 28 February 2022, available at https://news.un.org/en/story/2022/02/1112962.

115 Ibid.

116 Ibid.

117 OHCHR (2022). Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights.19 August. A/HRC/50/55.

118 Access Now (2022), The return of digital authoritarianism. Internet shutdowns in 2021. April. A #KeepItOn report. https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

119 Ibid.

120 DW Akadamie, "Digital authoritarianism: a global phenomenon". 17 March 2022, available at https://www.dw.com/en/digital-authoritarianism-a-global-phenomenon/a-61136660.

121 UN HCR (2021). Ending Internet shutdowns: a path forward. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association. 15 June. A/HRC/47/24/Add.2.

122 OHCHR (2022). Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights.19 August. A/HRC/50/55.

123 Ibid.

124 Hate speech is defined as "any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor", according to the United Nations strategy and plan of action on hate speech.

125 No distinction is made between artificial general intelligence (AGI) and narrow artificial intelligence (NAI). AGI refers to an AI system capable of doing and learning anything a human could (also called "deep learning") whereas NAI describes an artificial intelligence system that is specified to handle a singular or limited task.

126 The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Special Rapporteur on minority issues, Special Rapporteur on freedom of peaceful assembly and of association, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and Special Rapporteur on freedom of religion or belief.

127 OHCHR, "UN experts highlight digital rights in conflict and humanitarian crises at RightsCon", 15 June 2022, available at https://www.ohchr.org/en/press-releases/2022/06/un-experts-highlight-digital-rights-conflict-and-humanitarian-crises.

128 Human Rights Council, Resolution 20/8 of 5 July 2012, Council resolutions 26/13 of 26 June 2014, 32/13 of 1 July 2016 and 38/7 of 5 July 2018.

129 See, as an example, Meta's violence and incitement policy. 24 February 2022. Available at https://transparency.fb.com/en-gb/policies/community-standards/violence-incitement/.

130 Access Now, "Updates: digital rights in the Russia-Ukraine conflict", 18 August 2022. Available at https://www.accessnow.org/digital-rights-ukraine-russia-conflict/.

131 e.g. #Bucha, #BuchaMassacre, #GenocideOfUkrainians, #RussianWarCrime, and the popular #StandWithUkraine.

132 See "Call for submissions: challenges to freedom of opinion and expression in times of conflicts and disturbances" of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Available at https://www.ohchr.org/en/calls-for-input/2022/call-submissions-challenges-freedom-opinion-and-expression-times-conflicts-and.

133 A/HRC/35/22 § 44.

134 A/HRC/47/24/Add.2. A/HRC/47/16. A/HCR/35/22. A/HRC/RES/47/16. A/HRC/50/55. A/HRC/48/31.

135 A/74/821§ 41.

rights to freedom of peaceful assembly and association[136] reaffirmed the applicability of human rights law and international law to digital technologies, echoing the commonly agreed principle that "the same rights that people have offline must also be protected online".[137] The UNESCO recommendations on the ethics of AI reaffirm the application of international law, human rights and the United Nations Charter principles to artificial intelligence.[138]

Yet trends over 2022 consistently demonstrated that state actors have frequently and systematically used internet shutdowns to limit, restrain and shrink the online space, "asserting control on the population",[139] reducing and/or hindering the enjoyment and application of human rights, and hiding human rights violations. In that respect, the 2022 Freedom on the Net report[140] observes that "global internet freedom declined for the 11th consecutive year [and that] free expression online is under unprecedented strain … with more governments arrest[ing] users for nonviolent political, social, or religious speech than ever before, officials suspend[ing] internet access in at least 20 countries, and 21 States block[ing] access to social media platforms". Other civil society actors noted that surveillance and control practices have been globally normalized with "authorities in at least 45 countries suspected of obtaining sophisticated spyware or data-extraction technology from private vendors".[141] Those uses of digital technologies, combined with AI systems to gather data, significantly increase the risks of unlawful and arbitrary intrusions and breaches of the right to privacy. The risks are even more real and high as interoperability, the level of granularity, the de-identification of data and triangulation of information can lead to the identification of private, sensitive and confidential information of potentially anyone—and without the individual being aware of the collect, use and reuse of their data. Additionally, such uses of data are not subjected to any limitation period, usually unnoticed and not (easily) traceable. This can lead to extortion, blackmail, harassment and any other future forms of exploitation of personal data.

Biometric systems add another layer of risks. Facial recognition systems and video surveillance are used at a massive scale for safety and police purposes, enabling States to collect more and more data in the public space. Some already existing facial recognition systems monitor the emotions and reactions of individuals with the belief that it is possible to infer someone's state of mind and beliefs based on its their facial expressions.[142]If considering the aggregated amount of data gathered with those various AI systems, the risk is very high that the technologies that are tracking, identifying, monitoring, controlling, influencing and putting groups and individuals under constant surveillance in public spaces will be used for political purposes. This can also lead to pre-emptive arrests based on the emotions supposedly detected. Moreover, unlike addressing other human rights offences and violations, once biometrics data have been stolen, leaked or stored, it is almost impossible to repair the damages.

The right of privacy of IDPs and beneficiaries of humanitarian aid and assistance is equally jeopardized by digital technologies and artificial intelligence. In June 2022,[143] the United Nations Special Rapporteurs jointly reaffirmed the "radical impact of digital technologies on any humanitarian response" and "the dependence on digital identity programs". The war in Ukraine was no exception. The war amplified the conversation around the risks and legal considerations surrounding digital humanitarian aid and assistance. Countries hosting IDPs have partnered with multilateral organizations to deploy digital and AI systems which mostly rely on the collection of sensitive biometrics data (e.g. facial geometry, iris scans and fingerprints) to use for central digital identity systems, cash-based interventions, biometric controls and identification at borders, the collection of data to reunite families and other tools; these have been widely deployed and scaled-up. Though the principle of "do no digital harm" has been long applied, the question of the integrity of the consent of individuals in dire circumstances is subject to interpretation and cannot be guaranteed. Individuals may lack data literacy or have the misperception that aid and assistance is conditioned to them consenting to the collection of their data. The lack of human rights–based policies and their inadequate implementation can also jeopardize beneficiaries' data rights. Cyberattacks have also targeted humanitarian actors: the exfiltration and hacking of data of NGOs jeopardizing the rights and safety of vulnerable groups[144] and attacks on communication systems which have disrupted the deployment of humanitarian aid and the dissemination of useful information to vulnerable populations, which can impact their safety.

In the context of war and conflict, another important issue is the impact on digital human rights and the rule of law of international sanctions and countermeasures taken by technology companies and States. International sanctions have often been called "collective punishment" or "blunt instruments" because they impact and harm populations with unintended consequences, sometimes hindering the provision of humanitarian assistance to those in need. In 2022, for example, the withdrawal of technology companies from the Russian Federation did not "tak[e] into account the negative impacts on human rights of people left behind. This le[ft] human rights defenders and civil society organizations with little access to the information and communication infrastructure vital for their work"[145] and led to complete isolation of both human rights actors and the population.

136 UN HCR (2021). Ending Internet shutdowns: a path forward. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association. 15 June. A/HRC/47/24/Add.2.

137 Human Rights Council, Resolution 20/8 of 5 July 2012, Council resolutions 26/13 of 26 June 2014, 32/13 of 1 July 2016 and 38/7 of 5 July 2018.

138 UNESCO recommendation on the ethics of artificial intelligence adopted on 23 November 2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137.

139 Access Now (2022), The return of digital authoritarianism. Internet shutdowns in 2021. April. A #KeepItOn report. https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

140 Freedom House (2021). Freedom on the Net 2021 Report. The Global Drive to Control Big Tech, available at https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf.

141 Ibid.

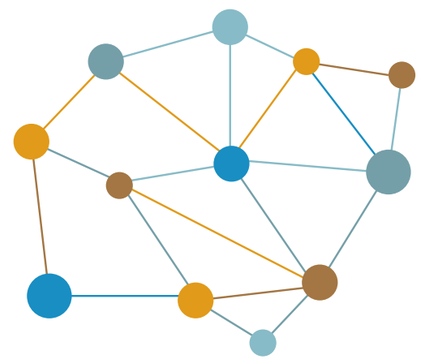
142 Facial emotional recognition systems have been developed in the education system to monitor the level of attention of students. They are also used to test customer reactions or during recruitment processes.

143 OHCHR, "UN experts highlight digital rights in conflict and humanitarian crises at RightsCon", 15 June 2022. Available at https://www.ohchr.org/en/press-releases/2022/06/un-experts-highlight-digital-rights-conflict-and-humanitarian-crises.

144 ICRC, "Cyber-attack on ICRC", 24 June 2022, available at https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

145 OHCHR, "Russia: UN experts condemn civil society shutdown", 13 July 2022, available at https://www.ohchr.org/en/press-releases/2022/07/russia-un-experts-condemn-civil-society-shutdown.

In this worldwide context, the international community and civil society have called for an increased human rights–based, transparent and accountable digital governance system that respects international human rights law and international humanitarian law. There have been renewed calls to safeguard humanitarian data.[146] The United Nations issued recommendations[147] reaffirming that "any restrictions should be guided by the objective of facilitating rights, rather than seeking unnecessary and disproportionate limitations on it",[148] that States bear the burden of justifying any restrictions, and reaffirming the vital importance of the respect of human rights online in democratic societies and for the rule of law. Regarding the justifications of restrictions, the United Nations also stressed that proportionate restrictions should be the least intrusive and that shutting down entire parts of communication systems can never be justified under human rights law,[149] echoing the Council of Europe.[150] The United Nations Special Rapporteur reaffirmed that companies, telecommunication providers and social media platforms' "human rights responsibilities apply fully"[151] in line with the United Nations Guiding Principles on Business in Human Rights, in the face of more constraints including internet shutdowns, throttling and increased State control. They should "seek to provide regular updates about the services affected or restored, the steps they are taking to address the issue and explanations after the fact … take innovative transparency measures, such as the publication of aggregate data and the selective withholding of information"[152] and cooperate with civil society.[153] In parallel, civil society has been very active monitoring and reporting human rights abuses and violations, monitoring internet shutdowns, launching initiatives (e.g. Open Observatory of Network Interference, #KeepItOn, Freedom online coalition) and organizing global multi-stakeholder forums, such as RightsCon.



146 Draft resolution 'Safeguarding Humanitarian Data'. Council of Delegates of the International Red Cross and Red Crescent Movement. 22–23 June 2022.

147 UN HCR (2021). Ending Internet shutdowns: a path forward. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association. 15 June. A/HRC/47/24/Add.2.

148 Ibid.

149 Ibid.

150 CM/Rec (2016) 4 on the protection of journalism and safety of journalists and other media actors.

151 UN HCR (2021). Ending Internet shutdowns: a path forward. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association. 15 June, § 55. A/HRC/47/24/Add.2.

152 Ibid., § 57.

153 Ibid., § 87.

Regional Trends

Regional trends have followed the same patterns and dynamics as global and national trends. Governments continued to invest in digital technologies and artificial intelligence systems to digitalize public services (e.g. e-government, digital identity, public transport, security, health), sometimes with the support of the European Commission, as in the Eastern Partnership, channelled through the EU4Digital Initiative.[154] Access to the internet has improved with 31 percent of individuals mostly satisfied with accessibility to public services via digital channels in the Western Balkans.[155] With regard to affordability, an ITU study[156] revealed that many countries have met affordability targets for 4G connectivity though "there remain significant populations of Europe that are unconnected. For example, 36% of the population in Central and Eastern Europe is unconnected, compared to 19% of Western Europe. In addition, 42% of 3 to 17-year-olds in Europe and Central Asia are unconnected at home, with clear impacts on educational outcomes and opportunities".[157] However, the pandemic has catalysed the rapid acceleration of both digitalization and connectivity.

Artificial Intelligence strategies continued to be initiated though most countries remain without a formal National AI Strategy.[158] The use of facial recognition and other biometric AI systems have been unequally deployed in the public space with the positions on the legitimacy and risks of such technologies differing between Central Asia, South Caucasus and Eastern Europe, and the Western Balkans and Türkiye. Facial recognition has been widely deployed in Central Asia and South Caucasus and Eastern Europe. In the Western Balkans, facial recognition is still very much questioned, and authorities do not admit to using it with the exception of Serbia. To date, "facial recognition technology is currently in use in 76% of countries in the Middle East and Central Asia, the second-largest share of any region".[159]

Partnerships between multilateral organizations (United Nations, European Commission, Council of Europe) and countries of the region have continued to support the deployment of digital technologies and artificial intelligence. In March 2022, Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine joined the European DIGITAL SME Alliance. The EU4Digital Facility completed in March the second release of e-Signature piloting with the participation of Armenia, Georgia and Ukraine. It enables eSignature interoperability across borders despite the remaining disparities between existing technological solutions and legislative frameworks.

154 EU4Digital, available at https://eufordigital.eu/.

155 Balkan Barometer, available at https://www.rcc.int/balkanbarometer/results/2/public.

156 The study was conducted under the umbrella of the regional initiative for Europe within the framework of accessibility, affordability and skills development for all to ensure digital inclusion and sustainable development, focused on the digital divide occurring in five Western Balkan states (Albania, Bosnia and Herzegovina, Montenegro, North Macedonia and Serbia) and three Eastern Partnership countries (Georgia, Moldova and Ukraine).

157 Ibid.

158 OECD.AI Policy Observatory, "National AI policies & strategies", available at https://oecd.ai/en/dashboards.

159 Surfshark, "The Facial Recognition World Map", available at https://surfshark.com/facial-recognition-map.

Regional cooperation mechanisms with China have also helped support digitalization and connectivity in Central Asian countries. In January 2022, China and five Central Asian countries renewed their commitment to the C+C5 cooperation mechanism, an agreement between China and five Central Asian countries: Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan. President Xi Jinping stated that "the two sides should speed up high-quality cooperation, and strengthen cooperation on artificial intelligence, big data, cloud computing and other high-tech sectors".[160] In June 2022, C+C5 was praised for the support provided by China during the COVID-19 pandemic in improving connectivity in the region and building strong infrastructure. This led to the signing of four documents including "an initiative to deepen cooperation in the field of connectivity and cooperation among China + Central Asia C+C5 countries, and an initiative for cooperation of China + Central Asia C+C5 countries in the field of data security".[161] These agreements are part of the Digital Skills Road (DSR) project launched in 2015. DSR is an umbrella project in the larger strategic Chinese plan of the Belt and Road Initiative (BRI), designed to export the Chinese global vision, technology governance,[162] technological influence[163] and its technological instruments.[164]

Regarding Chinese technological influence, it is reported that "Chinese telecom giants such as Huawei and ZTE, being the largest telecommunication suppliers and major providers of 5G technologies, have been successfully realizing their goal to dominate the 5G market worldwide. Leading Chinese surveillance companies such as Hikvision, Dahua and Huawei are among the major providers of surveillance services and technology among developing nations. The Chinese BeiDou Navigation Satellite System was created as an alternative to the United States' Global Positioning System (GPS), with the purpose of creating a world-class navigation satellite system to ensure the country's national security and promote global satellite navigation development by creating the Global Navigation Satellite Systems (GNSS). TikTok app, smartphone producers such as Oppo, OnePlus, Xiaomi, Huawei, ZTE, drone makers such as DJI and XAG are in great demand, especially among developing nations".[165] China and the Cooperation of Central and Eastern European Countries (the 17+1 Group)[166] is another cross-regional cooperation mechanism with an emphasis on digital and green investment and operations aligned with European Union rules to help promote their European integration process, while offering an opportunity to diversify their trade routes. Compared to the C+C5 cooperation mechanism, the expectation of the 17+1 mechanism has not fully materialized with a low level of investment,[167] fewer partnerships with Chinese technology companies[168] (e.g. Huawei technology partnerships with Bosnia and Herzegovina and Montenegro, the Huawei and Albania deal for 4G network infrastructure) and public opinion concerns about cooperation with China (e.g. EU-specific cybersecurity standards)[169] and China's intentions.[170]

The Chinese Institute of International Studies commented that "The main concern is that Chinese companies may obtain sensitive data in the field of digital cooperation".[171] The war in Ukraine[172] has reinforced scepticism with countries realizing the "considerable political and security risks stemming from cooperation with China … In an essence, while economic preferences may be debated and restructured as politically fitting, security is non-negotiable".[173] The same security reasons have prompted some Central and Eastern European countries (Georgia, Moldova and Ukraine) to accelerate their applications to join the European Union.

The level of freedom[174] on the internet varies from free[175] and partly free[176] to not free[177] with differences related to state control and surveillance and human rights violations and abuses. In Eastern Europe, Central Asia and Türkiye, civil society "signal[s] increasingly aggressive attempts by state authorities to assert control over populations, with broad censorship and network disruptions laying the groundwork for future aggression".[178] Internet shutdowns were also reported in the region.[179] Shutdowns occurred during political unrest and protests[180] "to thwart and disarticulate the protest itself", preventively to destabilize or prevent the planning of peaceful protests, but also "to hide the human rights violations that are commonly linked to security forces' crackdown on protesters".[181] Shutdowns also occurred during electoral processes.[182] Mobile internet shutdowns[183] were frequently imposed; throttling, blocking VPNs and blocking specific platforms were methods used[184] with a direct and significant impact on human rights. According to the BIRN report,[185] the most common violations in Southern and Eastern Europe were related to expression and activities on the internet, manipulation and propaganda in the digital environment, and information security breaches. These included hate speech against certain groups, minorities and migrants,[186] and also included the emergence of new cyberattacks (fraud, phishing scams, hackers) and threats against e-services to obtain personal data. For instance, digital banking and postal services were attacked in Serbia to scam customers.

Likewise, regional threats and trends in times of war and conflict echoed those across the globe. Cyberattacks against governmental authorities (ministries of foreign affairs,[187] national databases, governments) and infrastructure[188] were launched and denounced by governments and technology companies.[189] In August and September 2022, a wave of significant cyberattacks targeted the Western Balkans and led to the first severing of diplomatic relations.[190] Assumptions were made that a State was behind such attacks.[191] These events clearly showed that there are new forms of foreign interference in times of war and conflict.

Humanitarian actors also deployed digital tools and programmes. They were assisted by a robust European digital infrastructure. For example, the UNCHR used cash assistance and biometrics to distribute and provide services and the Ukrainian government used the existing smartphone application 'Diia' to send financial assistance to IDPs. The IOM[192] took advantage of its presence in the Eastern Europe region to facilitate the safe movements of people across borders with the Republic of Moldova. Moldova worked in coordination with the IOM and Romania to facilitate the safe movement of people through a "green corridor", while Türkiye sent mobile kitchens and 82 truckloads of humanitarian assistance. At the same time, cyberattacks were launched to disrupt humanitarian efforts. Concerns were also raised about the right to privacy and the protection of data of IDPs, and consequently the risks of misuse, data leaks and coercion on humanitarian actors.

160 The People's Republic of China News. "China, Central Asian countries vow to build community with shared future", 27 January 2022, available at http://english.www.gov.cn/news/topnews/202201/27/content_WS61f1f7c6c6d09c94e48a457c.html.

161 The People's Republic of China News. "FM attends third C+C5 foreign ministers' meeting in Kazakhstan", 9 June 2022, available at http://english.www.gov.cn/statecouncil/wangyi/202206/09/content_WS62a13e04c6d02e533532be21.html.

162 ZAWYA, "BRI: Digital know-how along China's BRI will set future global tech standards", 2 January 2022, available at https://www.zawya.com/en/business/bri-digital-know-how-along-chinas-bri-will-set-future-global-tech-standards-oj9bn5hc.

163 Richard Ghiasy and Rajeshwari Krishnamurthy, "China's Digital Silk Road and the Global Digital Order", The Diplomat, 13 April 2021. Available at https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

164 Albina Muratbekova, "China's post-pandemic Digital Silk Road", Eurasian Research Institute, available at https://www.eurasian-research.org/publication/chinas-post-pandemic-digital-silk-road/.

165 Ibid.

166 Referred to as China-CEEC or the 16+1 (or 17+1) Group, it includes Albania, Bosnia and Herzegovina, Montenegro, North Macedonia and Serbia.

167 Ivana Karaskova, "How China lost Central and Eastern Europe", Mercator Institute for China Studies (MERICS), 22 April 2022, available at https://merics.org/en/short-analysis/how-china-lost-central-and-eastern-europe.

168 China Institute of International Studies-CIIS. The Status and Prospects of China-CEECs Digital Economy Cooperation Report. April 2022.

169 Ibid.

170 Marta Makowska, "China's Digital Authoritarianism vs. EU Technological Sovereignty: The Impact on Central and Eastern Europe", Council on Foreign Relations, 19 May 2022, available at https://www.cfr.org/blog/chinas-digital-authoritarianism-vs-eu-technological-sovereignty-impact-central-and-eastern.

171 China Institute of International Studies (CIIS). The Status and Prospects of China-CEECs Digital Economy Cooperation Report. April 2022.

172 Ivana Karaskova, "How China lost Central and Eastern Europe", Mercator Institute for China Studies (MERICS), 22 April 2022, available at https://merics.org/en/short-analysis/how-china-lost-central-and-eastern-europe.

173 Ibid.

174 Freedom House, Freedom on the Net, "Countries", available at https://freedomhouse.org/countries/freedom-net/scores.

175 Armenia and Georgia.

176 Kyrgyzstan and Ukraine.

177 Azerbaijan, Belarus, Kazakhstan, Türkiye and Uzbekistan.

178 Access Now (2022), The return of digital authoritarianism. Internet shutdowns in 2021. April. A #KeepItOn report. https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

179 Ibid.

180 Kazakhstan and Turkmenistan.

181 Access Now (2022), The return of digital authoritarianism. Internet shutdowns in 2021. April. A #KeepItOn report. https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

182 Belarus.

183 Kazakhstan and Turkmenistan.

184 Kazakhstan, Tajikistan, Turkmenistan and Uzbekistan.

185 BIRN (2021), Annual Digital Rights Report 2021 – Online intimidation: controlling the narrative in the Balkans. 31 December, available at https://balkaninsight.com/wp-content/uploads/2021/12/ONLINE-INTIMIDATION-CONTROLLING-THE-NARRATIVE-IN-THE-BALKANS-1.pdf.

186 In August 2021, according to the BIRN Annual Digital Rights Report (ibid.), an Instagram account titled "Borca Against Migrants" posted insults against the migrant population in the Borca neighborhood in Belgrade, asking users to submit information about migrants.

187 Ukraine.

188 Albania.

189 Microsoft Threat Intelligence Center and Microsoft Digital Security Unit, "ACTINIUM targets Ukrainian organizations", 4 February 2022, available at https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/.

190 See page 24 under the paragraph for Albania.

191 James Pearson, "Hackers are targeting European refugee charities -Ukrainian official", Reuters, 3 March 2022, available at https://www.reuters.com/world/europe/hackers-are-targeting-european-refugee-charities-ukrainian-official-2022-03-23/.

192 IOM (2022), Ukraine crisis 2022: 6 months of response, available at https://www.iom.int/sites/g/files/tmzbdl486/files/situation_reports/file/IOM-Ukraine-Regional-Response2022-6-Month-Special-Report.pdf.

Conclusion

In the current global and regional contexts, peace will be sustained globally if we protect, support and uphold human rights standards in relation to digital technologies and artificial intelligence in times of war and conflicts, and beyond—throughout the digital and AI cycles of conception, implementation, deployment and scaling up.

In addition to the recommendations made in the second part of this report, and in alignment with the United Nations Sustainable Development Goals, the following recommendations should be taken into consideration when addressing the threats, challenges and opportunities of digital technologies and artificial intelligence in relation with human rights, especially in times of war and conflict:

Respect and abide by international human rights law, international law and international humanitarian law in all circumstances.

UNDP should:

- Continue to develop partnerships for digitalization and artificial intelligence with a human rights and risk proportionate approach.
- Continue to develop partnerships for digitalization and artificial intelligence abiding by the "do no digital harm" principle in the humanitarian context and sharing the policies and methodologies developed by the United Nations and its innovation toolkit.
- Continue to monitor trends and threats in the region to provide technical guidance on international normative standards.
- Contribute to the dissemination of the work of the Special Rapporteur and Member States on challenges to freedom of expression in times of armed conflict to clarify the notions of state propaganda, information, disinformation, fake news and other relevant notions and provide advice to States in the region to align their legal and policy frameworks considering their local context.
- Continue to provide a platform for multi-stakeholder engagement with all stakeholders promoting an inclusive debate between States, the private sector, civil society and human rights groups.

States should:

- (Re)affirm engagement in the principle of "do no digital harm" transferring the international humanitarian principles of neutrality, impartiality, humanity and independence to the digital era.
- Apply and abide by the responsibility to protect by developing safeguards to avoid the sale, use, reuse or any other form of exploitation of data of citizens by a third party.
- Apply strictly international human rights law (offline and online):
    a. Strictly apply the principle of necessity, proportionality and non-discrimination.
    b. Condemn systematic and/or generalized digital tools and tactics to limit, hinder or deny the effective exercise and enjoyment of any human rights.
    c. Clearly define and legally frame any exception in relation with public order, public safety and national order (see a and b).
    d. Establish strict safeguards.
- Systemically conduct needs assessments and consequently refuse to implement and deploy technologies that are not necessary and/or present high risks for human rights (using the proportionate risk approach). This includes technologies and tools used in public spaces.
- Systemically and regularly conduct human rights assessments and monitoring, and adapt digital and AI systems accordingly, including for humanitarian tools and systems.
- Obtain and ensure informed consent of users, e.g. citizens, civilians and beneficiaries.
- Ensure adequate and effective remedies.
- Develop and invest in highly effective cyberdefence systems to protect governments, public services, the personal data of citizens and critical infrastructure.
- Systemically adopt and apply a human rights and risk-based approach in national strategies, development plans and all relevant policy documents at the national, regional, local and project level.
- Collaborate with civil society on law making, policymaking and best practices.
- Continue to collaborate with private actors, especially in relation to the use of information in times of war and conflict.

Business enterprises should:

- Actively engage with international bodies, national authorities and civil society on online content moderation in times of conflict and war.
- Develop clear online content policies in times of conflict and war, clarifying the concepts of state propaganda, information, disinformation, fake news and other relevant notions in alignment with the recommendations of the Special Rapporteur on freedom of expression and with international human rights, international law and international humanitarian law.
- Refrain from taking measures (e.g. shutting down platforms, deleting posts) that increase the vulnerabilities of populations affected by conflict and war.

Civil society, media and NHRIs should:

- Continue to play an active role in monitoring and reporting human rights developments and violations and holding States accountable, especially concerning remedies.
- Continue to play an active role in monitoring online content policies of technology companies, engaging with them to adapt their policies to regional and national contexts in compliance with international human rights and international humanitarian law.
- Continue to actively report on any violations or the inadequacy of public and private laws and policies on online content.
- Engage actively in research, advocacy and policymaking in relation to the concepts of misinformation, disinformation, propaganda and other relevant notions in times of conflict, war and disturbances.
- Engage and participate with the Special Rapporteur and Member States on challenges to freedom of expression in times of armed conflicts to clarify notions of state propaganda, information, disinformation, fake news and other relevant concepts.
- Continue to inform the general public of their rights and the different mechanisms available to them.

Stakeholder engagement, public awareness and civil society capacity-building on digital technologies and AI

UNDP should:

- Continue to facilitate meetings between government officials, innovation communities and civil society.
- Continue to engage in capacity-building of NHRIs, civil society and media.

States should:

- Make continuous efforts to inform citizens of their rights in an effective way using various support and dedicated webpages on the various relevant authorities.
- Continue to launch campaigns to raise awareness on digital technologies and artificial intelligence among the general public in ways that resonate with the local context and communities.

Civil society, media and NHRIs should:

- Continue to build internal capacity on the specific issues raised during times of conflict, war and disturbances.
- Continue to build internal and external capacity engaging in workshops and trainings on human rights and digital technologies in times of conflict, war and disturbances.
- Continue to monitor digital regulations and initiatives and hold States to account on their compliance to international and constitutional standards.
- Continue to launch campaigns to raise awareness on digital technologies and artificial intelligence among the general public in ways that resonate with the local context and communities.

Business enterprises should:

- Continue to make their content policies clearly and easily accessible, with the relevant mechanisms to signal abuse.
- Continue to monitor and limit hate speech and calls for violence, especially in times of conflict and war, according to international law and international standards.
- Refrain from shutting down platforms and/or services, which further isolate vulnerable populations, especially in times of conflict and war.

Annex A:
International instruments applicable to privacy and data protection

Universal Declaration of Human Rights

The United Nations Universal Declaration of Human Rights (UDHR) of 1948 was the first international legal instrument in which the individual's right to privacy was articulated. Article 12 of the Declaration states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[193]

International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR), which was adopted by the UN General Assembly in 1966 and has to date been ratified by 168 States, provides in Article 17 that: "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states: "everyone has the right to the protection of the law against such interference or attacks."[194] General Comment No. 16 of the UN Human Rights Committee on Article 17 (Right to Privacy) noted that, in the view of the Committee, "the expression 'arbitrary interference' can also extend to interference provided for under the law". General Comment No. 16 of the UN Human Rights Committee also provides further guidance as to the scope of the right to privacy enshrined in Article 17 of the ICCPR with regard to the obligations of public authorities engaged in data collection and processing activities.[195]

Furthermore, the UN General Assembly Resolution of 28 December 2020 on "The Right to Privacy in the Digital Age" also underscores the importance of the requirement to consider ICCPR Article 17 on the Right to Privacy in respect of the principle of non-discrimination (Article 26 of the International Covenant on Civil and Political Rights), which provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with Article 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks", as well as with Article 2, paragraph 1.[196]

Organisation for Economic Co-operation and Development

Privacy Guidelines

The Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines represent the first attempt to deal with transborder data flows from a global perspective. Adopted in 1980, the 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' are a non-binding set of principles that OECD Member countries may enact and have the dual aim of achieving acceptance of certain minimum standards on privacy and personal data protection, and of eliminating, as far as possible, factors which might induce countries to restrict transborder data flows. The OECD 1980 Privacy Guidelines established the first international set of privacy principles emphasizing data protection as a condition for the free flow of personal data across borders.[197] These OECD guidelines were intended to assist countries with drawing up national data privacy policies.

In 2011, an Expert Group was convened by the OECD to review the Guidelines. It ultimately recommended that the Guidelines be updated in specific key areas. Of particular note is that the review underscored that the core eight basic principles at the heart of the Guidelines be retained without amendment. In July 2013, the OECD Council adopted a revised 'Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data', following the recommendations given by the Expert Group.[198] With this 2013 update, the guidance now provides for a focus on implementation at the national level based on a risk management approach and improving interoperability between national privacy strategies,[199] and identifies specific principles for countries to take into account in establishing national policies.

Council of Europe

Convention for the Protection of Human Rights and Fundamental Freedoms

The formation of the Council of Europe (COE) in 1949 was followed by the adoption of the European Convention on Human Rights (ECHR) in Rome in 1950, which entered into force in 1953.[200] The Council of Europe has a genuine pan-European dimension. All members of the Council of Europe are signatories to the Convention for the Protection of Human Rights and Fundamental Freedoms.[201] Article 8 of the ECHR guarantees the right to respect for private and family life, home and correspondence.

Council of Europe

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

In 1981, the Council of Europe enacted its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (commonly referred to as 'Convention 108'). At the time of this study, it has been ratified and acceded to by 42 countries. The Convention is also open for signature by countries that are not Member States of the Council of Europe. While Convention 108 differs from the OECD Guidelines in a number of significant respects (for example, its binding character and its treatment of sensitive data and application to automated processing), the foundational principles of the two instruments exhibit a great deal of consistency.[202]

Convention 108 states that "The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')."[203] Those drafting Convention 108 selected language of a broad scope; in particular, the definition of "personal data" being "any information relating to an identified or identifiable individual",[204] while "automatic processing" is framed as the automation in whole or in part of "storage of data, carrying out of logical and/or arithmetical operations on those data, [or] their alteration, erasure, retrieval or dissemination."[205]

The Convention constituted the first international treaty on data protection of a legally binding nature. Convention 108 envisages binding principles addressing data quality (Article 5), data security (Article 7) and special categories of data (Article 6). Furthermore, the treaty is also progressive in its articulation of additional safeguards for data access rights (Article 8).[206] Article 8 of the Convention is particularly noteworthy because it articulates the right of the data subject to establish the existence and main purposes of an automated personal data file, confirm whether personal data relating to the data subject are stored in the file; to review the data and, where appropriate, to rectify or erase the data, in conjunction with establishing the right of the data subject to a remedy where there is a failure in compliance with other rights granted by the instrument.

Council of Europe

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows

Also relevant in the context of data protection and transborder data flows is Treaty 181 of the Council of Europe, which provides further refinement of provisions pertaining to the automatic processing of personal data regarding supervisory authorities and transborder data flows.[207]

The Convention is intended to improve implementation and safeguard mechanisms for the protection of personal data and privacy by improving the original Convention of 1981 (ETS No. 108) in two principal areas. First, it provides for the setting up of national supervisory authorities (most commonly, regulatory bodies such as Data Protection Agencies) responsible for ensuring compliance with laws or regulations adopted in pursuance of the Convention, concerning personal data protection and transborder data flows. The second refinement concerns transborder data flows to third countries. In accordance with the provisions of Convention 181, data may only be transferred if the recipient State or international organization is able to afford an adequate level of protection.[208]

193 United Nations, Universal Declaration of Human Rights (UDHR), 10 December 1948.

194 UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at http://www.refworld.org/docid/3ae6b3aa0.html.

195 See: UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. Available at http://www.refworld.org/docid/453883f922a.

196 UN, UN General Assembly Resolution, The Right to Privacy in the Digital Age – Report of the Office of the United Nations High Commissioner for Human Rights, A/RES/68/1670 of 21 January 2014, p. 12, para. 36.

197 OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

198 OECD, "OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data", as amended on 11 July 2013. Also see Fred H. Cate, Peter Cullen and Viktor Mayer-Schönberger. "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines." (OII, 2014), available at https://www.oii.ox.ac.uk/wp-content/uploads/2022/02/Data_Protection_Principles_for_the_21st_Century.pdf.

199 OECD, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," amended 1 July 2013, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

200 Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005), available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005. All Council of Europe Member States are party to the European Convention on Human Rights and new members are expected to ratify the convention at the earliest opportunity. The following States are parties to the Convention: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Montenegro, North Macedonia, the Republic of Moldova, Serbia and Türkiye. See the full list of members at https://www.coe.int/en/web/portal/47-members-states.

201 Relevant to this report, the Member States include Albania, Azerbaijan, Bosnia and Herzegovina, Montenegro, North Macedonia, the Republic of Moldova, Serbia, Türkiye and Ukraine.

202 The eight principles set out by the OECD are: 1) collection limitation; 2) data quality; 3) purpose specification; 4) use limitation; 5) security safeguards principle; 6) openness principle; 7) individual participation; and 8) accountability. See OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

203 Council of Europe – ETS no. 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, Article 1. Note: The Convention entered into force on 1 October 1985.

204 Ibid., Article 2(a).

205 Ibid., Article 2(c).

206 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data, and which seeks to regulate at the same time the trans-frontier flow of personal data. In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on them and, if necessary, to have it corrected. See further: COE, Details of Treaty No.108, available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

207 COE, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No. 181), available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181.

208 The signatory States that are relevant to this study are Albania, Armenia, Bosnia and Herzegovina, Georgia, North Macedonia, the Republic of Moldova, Serbia and Ukraine. See further: COE, Chart of signatures and ratifications of Treaty 181, available at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=181.

Council of Europe

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

In the 35 years that have elapsed since Convention 108 was opened for signature, the Convention has served as the foundation for international data protection law in more than 40 European countries. While the core principles contained in the Convention have stood the test of time with its principle-based and technology-neutral approach, the Council of Europe considered it necessary to modernize this landmark instrument in the sphere of data protection.[209] The modernization of Convention 108 pursued two key objectives: to tackle challenges resulting from the use of new information and communication technologies, and to further strengthen the Convention's effective implementation. The Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, commonly referred to as Convention 108+, from its entry into force, shall be considered an integral part of the Convention as amended.[210]

Council of Europe

Convention on Cybercrime

In November 2001, the Convention on Cybercrime was opened for signature in Budapest, Hungary.[211] Referred to most frequently as the 'Budapest Convention', it remains the most relevant international agreement on cybercrime and electronic evidence to date and, through reconciling effective criminal justice and human rights safeguards, it provides for the criminalization of offences against and by means of ICT, tools for procedural law to secure electronic evidence and for international cooperation among Parties. To date, the Budapest Convention remains the most relevant binding international treaty on cybercrime and electronic evidence.[212] The Convention covers a broad range of offences, and its provisions are applicable to a broad range of concerns including botnets, phishing, terrorism, identity theft, malware, spam, distributed denial-of-service and critical infrastructure attacks, election interference and cyber violence. On 28 May 2021, a draft of the Second Protocol to the Convention was approved. It will enhance cooperation and disclosure of electronic evidence and provides for several data protection safeguards. The Protocol was finalized and adopted in November 2021 and was opened for signature in May 2022.

European Union

Extraterritorial implications of the GDPR

The EU's General Data Protection Regulation (GDPR), effective as of May 2018, establishes rules for EU members and also applies to the European Economic Area (EEA), which includes all EU countries plus Iceland, Liechtenstein and Norway. The GDPR is a comprehensive data protection and privacy regime that builds on previous EU law governing the protection of personal data. The GDPR grants new rights to individuals to control personal data and creates specific new data protection requirements, including provisions that carry extraterritorial implications, particularly in the context of transborder data flows.[213]

Several rights and provisions of the GDPR are of particular relevance for AI-based profiling and decision making (Recital 71; Articles 5, 12–15, 22, 25 and 35). The GDPR also establishes recourse for algorithmic decisions, offering individuals the right to a human rights review of a decision made by an automated AI-based system. An evaluation of the GDPR by the EU in 2020 recognized it as a flexible, technology-neutral and future-proof tool. However, it acknowledged some challenges lie ahead in clarifying how to interpret and apply the principles to specific technologies such as AI.

Also relevant in the context of the EU's regulatory framework for data protection and privacy are the Commission's adequacy decisions. The European Commission has the power to determine, on the basis of Article 45 of Regulation (EU) 2016/679, whether a country outside the EU offers an adequate level of data protection. The European Parliament and the European Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation. The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.[214] In effect, any transfers to the country in question will be assimilated to intra-EU transmissions of data. The European Commission has, to date, not recognized any of the countries within the scope of this study as providing adequate protection.[215]

209 Signatories to the Protocol, found in the chart of signatures and ratifications of Treaty 223, are Armenia, Bosnia and Herzegovina, North Macedonia and Serbia. See further: Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

210 COE (2018). Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

211 Council of Europe, Convention on Cybercrime (ETS No. 185), available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

212 Signatory States relevant to this study are Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Montenegro, North Macedonia, Serbia, Türkiye and Ukraine. Also see COE, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY", available at https://www.coe.int/en/web/cybercrime/parties-observers.

213 The GDPR applies to entities outside the EU that offer goods or services (for payment or for free) to individuals in the EU or monitor the behaviour of individuals in the EU. See further: European Commission, "Rules on international data transfers", available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en.

214 An adequacy decision permits a cross-border data transfer outside the EU, or onward transfer from or to a party outside the EU without further authorization from a national supervisory authority (Article 45(1), GDPR).

215 European Commission, "Adequacy decisions – How the EU determines if a non-EU country has an adequate level of data protection", available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.