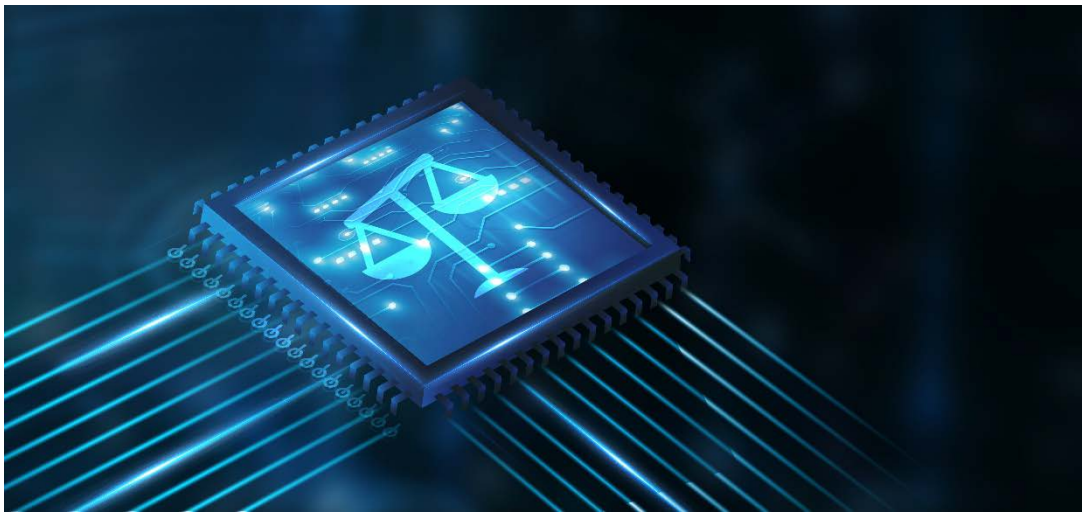
STUDY

Requested by the DROI subcommittee

European Parliament

# Digital technologies as a means of repression and social control



@Adobe Stock


Authors:

Dorota GŁOWACKA, Richard YOUNGS, Adela PINTEA, Ewelina WOŁOSIK

European Parliament coordinator:

Policy Department for External Relations

Directorate General for External Policies of the Union



PE 653.636 - April 2021


EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

STUDY

# Digital technologies as a means of repression and social control

## ABSTRACT

The proliferation of new and emerging technologies over the past two decades has significantly expanded states' toolkit for repression and social control, deepening human rights problems. While these technologies still have the potential to positively enhance democratic values and human rights, they are now also actively deployed and shaped by many repressive regimes to their own strategic advantage. Globally and regionally, efforts have been made to tackle the challenges that digital technologies pose to human rights, but a lot remains to be done. The EU must enrich global legal and standard-setting efforts, as well as improve its own core foreign policy instruments. The EU's foreign policy toolbox has become more comprehensive in the last several years, with the addition of a number of different strands to its efforts against 'digital authoritarianism'. The challenge related to the use of digital technologies by authoritarian regimes has continued to deepen, however. The EU must therefore continue to find ways to fine-tune and add to this toolbox. A core finding that runs through this report is that the EU has undertaken many valuable and well-designed policy initiatives in this field, but still has to decide whether tackling digital repression is a core geopolitical interest at the highest political level.

EP/EXPO/DROI/FWC/2019-01/LOT6/R/04
April 2021 - PE653.636

EN

## AUTHORS

- Dorota GŁOWACKA, Panoptykon Foundation, Poland;
- Richard YOUNGS, Senior Fellow, Carnegie Europe, Brussels & Professor of International Relations, University of Warwick, UK;
- Supporting researchers: Adela PINTEA, Ecorys, Poland; Ewelina WOŁOSIK, Ecorys, Poland;
- Reviewers: Christoph O. MEYER, Professor of European & International Politics, King's College London; Adamantia RACHOVITSA, Assistant Professor of International Law, University of Groningen, Netherlands; Aleksandra DUDA, Ph.D., Ecorys, Poland;

## PROJECT COORDINATOR (CONTRACTOR)

- Joanna SMĘTEK, Ecorys, Poland



This study was originally requested by the European Parliament's Subcommittee on Human Rights.





## CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Marika LERCH, Policy Department for External Policies

Editorial assistant: Daniela ADORNA DIAZ

Feedback is welcome. Please write to marika.lerch@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu



## VERSION

English-language manuscript completed on 23 April 2021.





This paper will be published on the European Parliament's online database, 'Think Tank'

ISBN: 978-92-846-8024-5 (pdf)
doi:10.2861/953192 (pdf)
Catalogue number: QA-05-21-111-EN-N (pdf)

ISBN: 978-92-846-8025-2 (paper)
doi:10.2861/6706 (paper)
Catalogue number: QA-05-21-111-EN-C (paper)

# Table of contents

# List of boxes



# List of tables



# List of figures

# Executive summary


**Study objectives and scope**

The main objectives of the study on digital technologies as a means of repression and social control were to provide:

- an overview of the normative framework as regards the human rights standards to be respected in the use and regulation of digital technologies, as established by regional and international human rights bodies as of 2020;
- an assessment of the existing EU policy framework and toolbox to respond to the use of digital technologies for repression and control in third countries;
- recommendations for EU institutions, and the European Parliament (EP) in particular, on how the policy framework and the toolbox could be further developed to take into account current geopolitical trends and challenges to the multilateral system.

The study focused specifically on situations outside of the EU, and the EU's external policy framework. EU internal policies and regulations were also referred to where these are relevant for bilateral and multilateral relations, however.

The main findings from this study derive from in-depth desk research and a series of interviews with representatives from institutions (EU, international), civil society and the private sector.

**Trends in the use of technologies for repression and social control**

The proliferation of new and emerging technologies has significantly expanded states' toolkit for repression and social control, leading to gradual deterioration of the level of human rights protection in this area over the past two decades. This process has been accelerated by the COVID-19 pandemic. While China remains the global leader in actively deploying and shaping new technologies to its own strategic advantage, harnessing these technologies to undermine human rights has occurred in all parts of the world, including less developed states to which opportunities to import 'off-the-shelf' solutions have become increasingly available.

The main global trend emerging in recent years is the expansion of ubiquitous data collection systems, including biometric surveillance, powered by artificial intelligence (AI) and algorithmic decision-making. It extends to a number of different fields, such as distribution of vital public services, healthcare, policing, administration of justice, education, finance, immigration, and commerce. Key challenges posed by those technologies include amplification of existing biases leading to possible discrimination and a lack of transparency resulting from a 'black box effect'. Other trends in the use of technologies for repression and social control identified in this paper include: (i) more 'traditional' tools and methods for repression and social control, including internet shutdowns and other network disruptions, as well as mass and targeted surveillance; (ii) an increasing use of the 'next generation repression toolkit', which encompasses practices that are more difficult to detect and hold accountable for (e.g. government hacking or state-sponsored online harassment campaigns); (iii) the expansion of digital authoritarian practices outside national borders through targeting diaspora or the export of surveillance technology. The rising power of a handful of tech companies which have become the gatekeepers of fundamental rights in the digital realm poses yet another significant challenge to those rights.

The risk of using new technologies to repress or control increases, in particular, in times of political tensions, elections, protests, demonstrations, armed conflicts or other kinds of crises, such as a pandemic. Among those most targeted are typically vulnerable groups, such as human rights defenders and other civil society activists, whistle-blowers, independent journalists, women, political opposition, as well as racial and ethnic

minorities. At the same time, expanding AI-driven data collection systems increasingly affects wider and harder to delineate categories of victims, among whom the most severely affected are the poor and the other most disadvantage groups in the society.

The identified trends reflect a number of wider mega-trends. First, regimes' use of state of emergency provisions related to different kinds of crises to justify long-term restrictions on fundamental rights. Second, 'technological solutionism', wherein technology is seen as the only viable option to resolve any social issue, often without appropriate fit-for-purpose and proportionality assessments. Third, 'surveillance capitalism', based on the invasive harvesting of personal data for profit by private actors, while at the same time allowing state authorities to exploit their services to their own advantage.

**Recent developments in the human rights framework**

Recent developments in the human rights framework reflect a growing awareness among the international community of how technologies affect societies in almost every part of our day-to-day lives. It has been widely recognised that general human rights treaties apply to the internet and other digital technologies and that design, development and deployment of those technologies are subject to a 'three-part test', i.e. must meet criterion of legality, pursue legitimate a aim, as well as be necessary and proportionate to achieve this aim. This means, in particular, that the use of digital technologies interfering with human rights must be always the exception, rather than the rule, must be provided in law, must be applied only in specific circumstances, and must involve the least restrictive means possible.

At the same time, the existing legal framework developed by intergovernmental bodies, both at the international and regional levels, such as the United Nations (UN), Council of Europe (CoE), the Organisation for Security and Cooperation in Europe (OSCE), Organization of American States (OSCE) and the African Union (AU), already specifically responds to many of the challenges identified above, both with its binding and (mainly) 'soft law' instruments. These standards are often complemented by the jurisprudence of the international courts.

Among the new and emerging technologies which may be used for repression and social control, a concern that dominates most current agendas of human rights organisations are threats posed by AI and algorithmic decision-making systems. Moreover, the human rights legal framework provides standards addressing problems such as internet shutdowns and other network disruptions, mass and biometric surveillance, government hacking, export of surveillance tools, and cyber harassment. Unfortunately, the continuing and increasing prevalence of these threats prevents them from disappearing from the human rights community's agenda. Furthermore, several bodies developed guidelines addressing many challenges posed by tech-focused responses to the COVID-19 crisis. The important next step however, is a further assessment of the expending pandemic-related measures' impact on human rights, ensuring they remain temporary, as well as continuing work towards more evidence-based recommendations on health emergency tools to prevent future abuse of surveillance technologies.

At the same time there are fields that should be further improved or addressed. The existing human rights framework, for instance, tackles new and emerging technologies being used for repression and social control in a fragmented way, often without taking into consideration interrelations between them[1]. Furthermore, while there has been increasing recognition that new and emerging technologies affect not only a wide range of civil and political rights but also economic, social and cultural rights, the latter should still be given more prominence on future human rights organisations' agendas. An ineffective application

[1] An example may be the recent UN Human Rights Council Resolution on Freedom of opinion and expression which fails to address the impact of surveillance technologies which cause significant chilling effect on freedom of expression (A/HRC/44/12).

of the human rights framework at the national level, with limited avenues for remedies for harms caused by its violations, also raises concerns. Another issue are gaps that are still present in the current level of protection, specifically when it comes to challenges posed by AI. This includes the lack of a comprehensive, specifically AI-tailored international legal instrument (even though there are already advanced debates on how this gap could be filled[2]), insufficient focus on the causes and impact of unintended bias and discrimination resulting from certain algorithmic and automated decision-making based on AI, or inadequacy of traditional notions of 'victim' status or 'harm' in the context of new, AI-driven technologies. Finally, a shift towards greater comprehensives has been also marked when it comes to the range of key actors who should be involved in responding to the challenges posed by new technologies. There has been an increasingly progressive approach in the legal framework towards human rights responsibilities of the private sector, particularly large online platforms, but also companies producing and selling surveillance equipment. However, due to the non-binding and non-ICT-sector specific character of the existing framework, largely based on the UN Guiding Principles on Business and Human Rights, its efficacy is currently limited. Ongoing efforts to develop a mandatory international legal instrument[3] to regulate human rights obligations with respect to private companies should therefore be encouraged.

**Assessment of the EU policy toolbox**

Overall, the EU has moved up a gear in its efforts to tackle digital challenges, but its external toolbox has improved mainly on select elements of this; in particular, it has focused on the use of digital technologies for repression against democracy and human rights actors within civil society, the export of surveillance equipment, and the transnational use of digital tactics against the EU itself. In terms of its effectiveness, the EU has retained (and even widened) its toolbox for human rights and democracy support against an extremely challenging global backdrop in recent years. The EU's direct financial support has also had a very clear, tangible impact in protecting many individual civil society activists from repression. The toolbox has become more comprehensive in the last several years, as the Union has added a number of different strands to its efforts against digital authoritarianism (i.e. digital-rights issues, digital elements in external funding for human rights and democracy, dialogues on online threats, EU cyber-security co-operation, a new cyber sanctions regime, building digital considerations into the EU's electoral missions, surveillance export rules). Still, it remains uncertain how relevant restrictive measures related to democracy and human rights are in response to the digital aspects of repression and rights abuses. It is also doubtful that focusing most of EU political aid to third countries on technical support to state institutions, or responding mainly to dramatic interruptions of democratic processes (such as obviously manipulated elections), rather than to gradual threats, are the optimal strategies for dealing with the specific challenges of digital repression.

At the same time, for all its improvements, it is clear that the EU toolbox does not yet fully cover all digital challenges that have arisen, and that more subtle forms of social control, advanced AI techniques or health-related controls have so far proven less amenable to being incorporated fully into foreign policy instruments. The challenge of digitally-led authoritarianism has continued to deepen, and regime attacks on democratic freedoms and human rights have become stronger and more far-reaching. Additionally, some of the emerging techniques of social control, health-system management, and advanced AI have not leant themselves easily to EU foreign policy tools. The EU itself has also devoted relatively limited funds for democracy and human rights, and it has not been willing to incur significant costs, in terms of letting trends in digital repression impact its commercial and strategic interests. In fact, the tensions between the EU's

[2] For example, the CoE established the Ad-hoc Committee on Artificial Intelligence (CAHAI), which was tasked to examine the feasibility of a legal framework (including possibly a binding instrument) for the development, design and application of AI. See, CoE CAHAI, 'Feasibility study', 2020.

[3] The elaboration of the Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises was mandated in 2014 by Resolution 26/9 of the UN Human Rights Council. The Second Revised Draft of the instrument was published in August 2020 and is undergoing negotiations. By the end of July 2021, a third revised draft text shall be presented, which will form the basis of negotiations later that year.

digital geopolitics and its commitments to advance democracy and human rights make it unclear whether all EU institutions and governments see the surge in digital authoritarianism itself as a geopolitical issue. All this makes it difficult to achieve the desired results of EU policies and to conclude that its toolbox is fully attuned to the specific features of digital repression and contemporary democratic backsliding.

**Recommendations**

In order to take the EU's fledgling efforts against digital repression further, the following recommendations, encompassing both the international human rights framework and the EU's foreign policy framework, are proposed:

a. Extending the global reach of EU values through the regulation of new technologies

- A strong push, by all actors in the EU, including the EP and the human rights community, for a comprehensive, binding legal instrument to address the specific challenges posed by AI-driven technologies.
- Using other EU standard-setting documents, such as a DSA-DMA package, the EDAP, or possible future instruments concerning mandatory due diligence for companies, to intensify multilateral efforts to strengthen the link between human rights and new technologies.

b. Putting more pressure on third countries

- Tightening the link between the EU's restrictive measures and digital repression by invoking 'essential elements' clauses, referring specifically to the need to respect 'digital freedoms and unhindered access to the internet', to be included in all new trade agreements.
- Widening the new Global Human Rights Sanctions regime by referring more explicitly and extensively to the multiple strands of digital repression covered in this study.
- Making digital repression a more central part of EU's high-level diplomacy and geopolitical strategies, and linking multilateral standard-setting forums and exercises to the EU's on-the-ground political developments.
- Providing more EU resources specifically to strengthen the rights-oriented monitoring of surveillance equipment exports.
- Using the EU's positive conditionality more systematically to leverage positive changes away from digital repression by responding with additional aid, trade, and strategic benefits to third-country governments that work with the Union to reform restrictive laws and incorporate international standards.
- Continuing and intensifying efforts to fuse the security and human rights elements of the EU's digital strategies in its array of cyber-security work, and connecting Stratcom's work to the core EU human rights and democracy support.

c. Putting more pressure on the private sector

- Increasing the EU's pressure on private company operations in third countries by pushing them to adhere to more rigorous standards within the EU itself (e.g. through a code or set of guidelines pertinent to companies' stances on internet shutdowns and acute forms of digital repression outside of Europe).
- Focusing more of the EU's attention on the problem of 'privatised censorship' (i.e. online platforms making decisions that have negative effects on the freedom of expression) in its work on protection of civil society from regimes' internet shutdowns and other network disruptions.

d. Increasing resources, funding, and capacity

- Increasing the EU's funding to digital empowerment projects (for example, by creating a 'human rights and technology fund', as suggested in the EP's 2015 EP resolution).
- Using the EP's position to get politicians (parliamentarians) engaged with civic initiatives as a means of amplifying their political impact, and to advocate for increased levels of support to the EED and other foundations.
- A more prominent role for the EP in pushing for the EU's range of human rights dialogues and positions in multilateral forums to address such developments.
- Directing more of the EP's support to a large-scale expansion of the EU's efforts to build digital elements into its EOMs – a natural area of partnership between the EP and EEAS.
- Investing more in the EU's capacity for monitoring necessary to identify and unpack overt and more subtle forms of digital repression and stipulate how they contribute to gross human rights violations of the type that might be liable to restrictive measures.
- Appointing a formal liaison or contact point for the EU, which links together the multiple cyber-security and human rights initiatives.
- Investing more EU resources in fostering wider coalitions of engagement, for example by including other actors in particular civil society and academia in the work on human rights and new technologies and allocating adequate (human) resources, thus closing the 'knowledge gap' between legal/human rights and technology experts.

# 1 Introduction

This section briefly presents the study objectives, scope, and methodological approach to the research process. It also provides brief definitions of such terms as 'digital technologies', 'repression', and 'social control' to delineate their meaning and place them in relation with, or differentiate them from, other relevant concepts used in this study. The latter include relatively recent concepts, such as 'digital rights', 'surveillance society', 'digital authoritarianism', or 'algorithmic governance'.

## 1.1 Objectives and scope of the study

Digital technologies, and technologic developments in general, play an increasingly important role in 'enabling and ensuring the fulfilment [of] and full respect for human rights and fundamental freedoms'[4], as they provide an additional platform for their fulfilment. At the same time, they can also be abused to consolidate power and violate various dimensions of human rights. The focus of this study is the use of digital technologies as a means of repression and social control, and the EU's external human rights policy options to tackle this threat. More specifically, this study aims to:

(1) provide an overview of the normative framework as regards the human rights standards to be respected in the use and regulation of digital technologies, as established by regional and international human rights bodies as of 2020;

(2) assess the existing EU policy framework and toolbox to respond to the use of digital technologies for repression and control in third countries;

(3) make recommendations for EU institutions, and the EP in particular, on how the policy framework and the toolbox could be further developed to take into account the current geopolitical trends and challenges to the multilateral system.

In order to address these, the study first explores the context of the problem of using digital technologies as a means of repression and social control, and highlights the main political and technical trends regarding human rights and digital technologies since the EP's 2015 'Study on Surveillance and Censorship: The impact of technologies on human rights'[5] and resolution on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries'[6].

These trends are reviewed in line with the following thematic areas:

(1) the expansion of widespread biometric surveillance and algorithmic decision-making;

(2) the emergence of public health surveillance systems;

(3) digital tools of information control;

(4) the next generation repression toolkit;

(5) transnational dimensions of digital repressions (Chapter 2).

Then, an overview and analysis of international human rights standards regarding digital technologies is presented, including standards set through relevant conventions and treaty bodies at international and regional level, advice and guidance documents adopted by special procedures and other relevant human rights mechanisms or bodies, as well as any relevant technical organisations. In this context, relevant

[4] European Parliament resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI)).
[5] Wagner, B., Bronowicka, J., Berger, C. and Behrndt, T., 'Surveillance and censorship: the impact of digital technologies on human rights', European Parliament, 2015.
[6] European Parliament, Resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI)).

international (governmental, private, or multi-stakeholder) initiatives that address and regulate human rights implications of digital technologies are also looked at (Chapter 3). A subsequent description and systematic assessment of the EU policy framework and toolbox for addressing the use of digital technologies for repression and social control in third countries covers:

(1) diplomatic tools at bilateral and international level;

(2) financial and technical support for reforms (governments, parliaments);

(3) support for human rights defenders and democracy activists;

(4) cooperation with the private sector, including in relation to technical standards;

(5) standard-setting in terms of businesses' human rights obligations (due diligence);

(6) trade/export controls.

These themes were assessed according to pre-defined criteria, such as comprehensiveness, effectiveness, efficiency, availability of expertise and resources, and adequacy of the instruments aimed at authoritarian regimes. How the instruments can be applied in countries in transition/ new democracies, or democratic countries at risk of backsliding, was also considered.

Finally, based on research findings, the study offers a set of conclusions, and proposes recommendations for EU institutions – the EP in particular – on how the policy framework and toolbox could be further developed to take into account current geopolitical trends and challenges to the multilateral system.

The research did not cover situations inside the EU and the EU's internal policy framework, as it was to look at external policies. Also, the use of digital technologies for creating or disseminating disinformation was given less weight, since it is covered by another research requested by the EP.

## 1.2 Definitions of key concepts

The study focuses on **digital technologies**, which are most commonly associated with smart, high-tech, internet-based solutions and tools. As these are subject to constant improvement and new technological applications, they may include, but are not limited to:

- Internet-based platforms and tools;
- telecommunication and video surveillance technologies (e.g. CCTV cameras);
- online databases and data pooling tools;
- Artificial Intelligence ('AI') based technologies;
- biometric technologies (e.g. facial recognition or finger/hand-scans);
- location technologies (e.g. Global Positioning System (GPS) or Geographical Information Systems (GISs);
- big data analytics and advanced algorithms;
- multi-level customer interaction and customer profiling[7].

In this paper, the term 'digital technologies' is used in subsequent sections interchangeably with notions such as 'new technologies' or 'emerging technologies'.

[7] United Nations, 'The Impact of digital technologies'.; Wood, D. M., et al., 'A report on the surveillance society', Surveillance Studies Network, 2006, p.7-9.; Geissbauer, R., Vedso, J. and Schrauf, S., Industry 4.0: Building the Digital Enterprise, PwC, 2016.

While acknowledging their wide application for the benefit of societies and human rights, the study is concerned with the use of digital technologies for repression and social control. Both terms are further discussed below, but they essentially entail a range of negative impacts on, or threats to, the enjoyment of human rights. In the context of the digital age, human rights are also referred to as '**digital rights**', and we use the terms interchangeably. Our understanding of digital rights thus follows a broad definition of the term as human rights that are applicable in the digital sphere. The digital sphere, in turn, 'covers both physically constructed spaces, such as infrastructure and devices, and spaces that are virtually constructed, such as online identities and communities'[8]. For practical reasons, in the following chapters, we highlight human rights which are (or have the potential to be) most visibly affected in the digital sphere. This includes civil and political rights (e.g. freedom of expression, the right to privacy, freedom of assembly, the right to public participation, and prohibition of discrimination), but also – in light of the increased application of digital technologies in various sectors of life – economic, social and cultural rights (e.g. the right to work, the right to social security, the right to the highest attainable standard of health, the right to education, and the right of everyone to enjoy the benefits of scientific progress and its applications). Given the universality, indivisibility, inter-relatedness and interdependence of all human rights, this study takes the view that digital technologies can negatively affect the full spectrum of currently recognised and newly emerging human rights.

Developments in the digital sphere have affected the functioning of states and ways in which authorities interact with citizens. The rapid growth and deployment of a new generation of AI algorithms and products has been playing an increasingly important role in public authorities' decision-making processes[9]. In an attempt to grasp this phenomenon, a concept of **algorithmic governance** has been developed, which applies to the usage of algorithms and AI-based technologies for governance purposes[10]. This emerging proliferation of algorithms in public policy- and decision-making contributes to the creation of large data sets, updated in real time, which 'are increasingly being used to nudge, bias, guide, provoke, control, manipulate and constrain human behaviour'[11]. In the context of human rights, algorithmic governance raises issues associated with the usage of surveillance systems, which are related, among others, to ethics, privacy and data collection, as well as fairness of data-based targeting and decision-making[12]. AI's automation and its potential to shape and change society raises additional questions about the efficiency, adequacy, and legitimacy of algorithm-based solutions[13].

Digital technologies can be misused as tools for human rights violations, including by governments and law enforcement bodies[14]. Such occurrences in the context of repressive regimes lead to the development of **digital authoritarianism** – a concept that can be understood as 'censorship going online'[15], which may include application of digital technologies to 'control, repress, and manipulate domestic and foreign

[8] Digital Freedom Fund.
[9] Wu, W., Huang, T. and Gong, K., 'Ethical Principles and Governance Technology Development of AI in China', Engineering, 6 (3), March 2020, pp. 302-309.
[10] Gritsenko, D. and Wood, M., 'Algorithmic governance: A modes of governance approach', Regulation & Governance, 2020.
[11] Danaher, J., et al., 'Algorithmic governance: Developing a research agenda through the power of collective intelligence', Big Data & Society, 4(2), 2017, pp. 1-2.
[12] Omer T. and Polonetsky J., 'Big data for all: Privacy and user control in the age of analytics' , Nw. J. Tech. & Intell. Prop. 11, 2012, pp. 251-253.
[13] Gritsenko D and Wood M., op. cit.; Sætra, H. S., 'A shallow defence of a technocracy of artificial intelligence: Examining the political harms of algorithmic governance in the domain of government', Technology in Society, 2020.
[14] European Parliament resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI)).
[15] Erixon, F. and Lee-Makiyama, H. 'Digital authoritarianism: Human rights, geopolitics and commerce', No. 5/2011, ECIPE Occasional Paper, 201, p. 4.

populations'[16] for the purpose of power consolidation[17]. Expanding synergies between different technologies allows repressive regimes to further strengthen surveillance, societal control, or even repression[18]. It may also bring about the usage of tools that are yet to be developed.

Digital authoritarianism is closely linked to the emergence of **surveillance society**, which is 'organised and structured by using surveillance-based techniques'[19]. Development of digital technologies not only enables wider and more intrusive access to information about people's movements, activities or preferences, but it also provides tools to maintain, sort, and categorise data for the purposes of public decision-making and **social control.** This is additionally reinforced by the ubiquity of surveillance technology and diverse range of data available[20]. An external aspect of social control could entail direct actions targeted at imposing desired behaviours of individuals and groups (as opposed to an internal social consensus that develops norms and behaviours to be followed). This can involve an active role of public institutions[21] and, in some cases, some form of coercion[22]. Therefore, it can play an important role in surveillance society where data-based institutional decisions can entail 'entitlement and access to benefits, work, products and services and criminal justice; health and well-being and movement through public and private spaces'[23]. This creates both incentives, and threats of possible 'soft punishments' for certain actions, thus providing very measurable tools for social control to reinforce or impose certain behaviours, values and norms[24]. Further development and solidification of the surveillance society can, in the long-term, impact (if it has not yet done so) the agency and the autonomy of individual choice[25].

Unlike social control, **repression** is associated with direct targeting of certain groups or individuals (based, for example, on the likelihood of them opposing the government). In these terms, digital technologies give regimes the power not only to react to online actions, but also to carry out online tracking and to prevent any possible actions against their rule in the very preliminary phases of organising dissent[26]. Techniques of repression can go beyond the online, into the real world. These could include:

- targeted censorship;
- social manipulation and harassment;
- cyber-attacks and bullying;
- purposeful internet shutdowns/slowdowns
- penalisation of online activity and targeted persecution against online users;
- extra-legal intimidation;
- imprisonment;

[16] Polyakova, A. and Meserole, C., 'Exporting digital authoritarianism: The Russian and Chinese models', Policy Brief, Democracy and Disorder Series, 2019, p. 2.
[17] Tiberiu, D. and Lupu, Y., 'Digital Authoritarianism and the Future of Human Rights', International Organisation, October 2020, pp. 10, 12.
[18] Wood, D.M. and Ball, K., (eds), 'A report on the surveillance society', Surveillance Studies Network, 2006, p. 8.
[19] Ibidem., p. 5.
[20] Ragnedda, M., 'Social control and surveillance in the society of consumers', International Journal of Sociology and Anthropology, 3(6), 2011, pp. 180-81.
[21] Ibidem.
[22] Ragenedda M. (2011), op. cit.
[23] Wood, D. M., et al. (2006), op.cit., p. 5.
[24] Ragnedda, M., op.cit.
[25] Gorwa, R., Binns, R. and Katzenbach, Ch., 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance', Big Data & Society, 7(1), 2020.
[26] Tiberiu, D. And Lupu, Y., op. cit.

- physical violence;
- other possible forms of harassment[27].

## 1.3 Note on methodology

The methodological approach to the research process included the following elements:

1. Revision of a wide range of available sources (no more than five-years-old), including:
   (i) official EU legal and policy documents;
   (ii) subject-relevant international human rights 'hard' and 'soft' law;
   (iii) subject-relevant publications by international organisations working on human rights and their bodies/mechanisms;
   (iv) academic and grey literature focused on digital technologies and rights;
   (v) jurisprudence;
   (vi) publications from established and independent media channels that display a high level of reporting on digital technologies and human rights.
2. Stakeholder consultations, based on topic guides tailored to different respondent categories, which targeted 23 respondents from the following groups[28]:
   (i) CSOs or their coalitions, working on human rights and digital technologies;
   (ii) EU institutions – in particular, representatives of the EC;
   (iii) CSOs or their coalitions, supporting human rights defenders (HRDs) and other groups affected by digitally-mediated repression and attempts at social control;
   (iv) representatives of the private sector, particularly ICT companies;
   (v) representatives of international organisations.[29]

The main goal of the interviews was to reach a better understanding of the practice, including how the EU foreign policy framework and toolbox are employed in selected third countries, and thus, to offer an "insider" perspective on the research subject.

Since the aspiration of the research was to see how the toolbox is applied in practice on the ground, some interviews had a specific country-focus. The selection of countries, which serve as practical examples, was based on the following criteria:

- extensive use of digital technologies for repression and social control;
- different levels of democratisation/freedom, including both authoritarian and democratic states, and those in transition;
- geographic distribution, meaning countries located in different continents and regions, representing different 'spheres of influence'.

[27] Feldstein, S., 'When it comes to digital authoritarianism, China is a challenge- but not only', War on Rocks, 2020.; Freedom House, 'Freedom of the Net 2020. China country report', 2020.; Freedom House, 'Freedom of the Net 2018', 2018, p. 24.
[28] No responses were obtained from representative of EU foreign policy think tanks and journalists working at the cross-section of human rights and digital technologies who were also contacted during the research process.
[29] Annex 1 presents the list of consulted stakeholders and topic guides.

While not fully representative, the choice of country examples aims to offer varied illustrations of trends and an opportunity to examine the application of different EU tools at country level. Overall, six countries from four continents (Africa, Asia, Europe, and South America) were selected as primary choices for more in-depth exploration. Some other criteria included participation in the Media4Democracy Technical Assistance Facility, application of EU foreign policy tools, and the presence of different trends in the employment of digital technologies for repression and social control.

In terms of its limitations, the research was centred on situations outside of the EU and on the EU's external policy framework, referring to EU internal policies and regulations only where relevant for bilateral and multilateral relations. Also, given its global geographic coverage (minus the EU), the study cannot claim to be exhaustive in terms of its review of trends and applications of the EU foreign policy toolbox. To address this, a deliberate effort was made to balance a broad analysis that included countries representing different continents and regions with attention to the areas where the most problems lie (i.e. countries, which lead the way, in terms of using digital technologies for repression and social control). These include, in particular, regimes in China and Russia, but also in other states and under other governments, which either follow in their footsteps, or implement their own agendas reliant on digitally enabled repression and/or social control.

# 2 Trends in the use of digital technologies for repression and social control

The following chapter will map the current global trends related to the use of new technologies for repression and social control. It will present an overview of how digital repression and social control have evolved in recent years, and how they currently work across the world – in particular, which regimes engage in such activities, and using what methods and tools. It will also explain how these efforts impact human rights, identify the most targeted or vulnerable groups, and highlight what the role of private sector is in the context of this phenomenon.

## 2.1 Expansion of widespread biometric surveillance and algorithmic decision-making

2020 has brought an unprecedented rapid upscaling of new technologies that support digital surveillance, in response to the COVID-19 pandemic. Governments across the world have deployed a range of new surveillance measures[30], often turning to advanced AI[31] and big data technologies, used not only for enhanced monitoring, but also increasingly to replace human judgment with algorithmic decision-making. Applications of these technologies may affect a particularly broad spectrum of human rights, ranging from the right to privacy, freedom of expression, freedom of peaceful assembly and association, and the right to non-discrimination to a number of social and economic rights, such as the right to health, work, and social security. While in principle all regions have witnessed the expansion of tech-focused responses to the pandemic, the countries that have been leaders in harnessing the most sophisticated technologies to combat COVID-19 were often the same states where intrusive, data-driven surveillance systems were in place even before the COVID-19 crisis began. The pandemic has therefore served as a catalyst for expanding those systems, while also preserving many pre-existing problems related to their use.

[30] Privacy International, 'Tracking Global responses to COVID-19', 2020.
[31] AI is a broad concept used in policy discussions to refer to many different types of technology. To date, there is no single definition of AI accepted by the scientific community. Definitions used by international organizations also vary. A comprehensive document on the definition of AI has been published by the High-Level Expert Group on AI mandated by the European Commission. See: AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines', 2019.

China is the country with the most advanced and pervasive surveillance system, built over the past two decades. It has also taken the most comprehensive and draconian approach to COVID-19 surveillance. Categorised as 'the world's worst abuser of internet freedom for the sixth year in a row' according to Freedom House's 'Freedom of the Net 2020' report[32], China has been the leader in the application of biometric surveillance, which is particularly ubiquitous in northwest China's *Xinjiang Uyghur* Autonomous Region[33]. Chinese authorities use biometric identification to track and restrict the movements and activities of the Uyghur through the use of facial recognition technology and mandatory collection of sensitive data, such as DNA samples and iris scans. It has also been established that this surveillance technology is used to arbitrarily place large numbers of Uyghurs and members of other ethnic groups in so-called 're-education camps' under the pretext of countering religious extremism, without detainees being charged or tried[34]. As noted by the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 'the picture that emerges [from the Uyghur Autonomous Region] is one of systemic ethnic discrimination, supported and indeed made possible by a number of emerging digital technologies'[35].

Algorithmic technologies based on big data have also been deployed in other parts of China. The authorities have been experimenting with machine learning and algorithmic decision-making in the service of the regime's politically repressive 'social management' policies[36]. Automated systems flag suspicious behaviour on the internet and, increasingly, in public spaces, using the world's largest security-camera network equipped with facial recognition, which enables tracking of individuals based on their physiological or behavioural characteristics. Data sets assembled through these surveillance efforts could feed into a 'social credit' system that creates an assessment of individuals' online activities and other personal data to monitor and rate individuals' overall behaviour. Being listed as a 'problematic' group or individual by municipal or provincial authorities, which are currently testing these systems, can result in

[32] Freedom House, 2020, op. cit., p. 2. The Report determines each country's internet freedom score on a 100-point scale, based on 21 indicators pertaining to free flow of information online and deployment of new surveillance technologies by public and private actors, which to great extent correspond to the concepts of 'surveillance' and 'social control' as used in this study.

[33] Xinjiang is an autonomous region in China which is home to a number of ethnic minorities, including the Muslin Uyghur minority, a Turkic ethnic group, recognized as native to the Region. The Chinese government has long carried repressive policies in Xinjiang, maintaining its actions are justifiable responses to a threat of extremism due to the East Turkestan independence movement (a political movement that seeks independence for the Region). These efforts have been dramatically scaled up since late 2016, when Communist Party Secretary Chen Quanguo relocated from the Tibet Autonomous Region to assume leadership of Xinjiang. At the same time human rights organisations and experts have presented evidence that these policies involve gross human rights violations, including mass arbitrary detention, torture, surveillance and mistreatment of Turkic Muslims in Xinjiang. See: Global coalition of more than 300 civil society organisations, 'Global call for international human rights monitoring mechanisms on China. An open letter to: UN Secretary-General Antonio Guterres, UN High Commissioner for Human Rights Michelle Bachelet, UN Member States', 2020.

[34] Much of the information collected through the surveillance systems is stored in a massive database, known as the 'Integrated Joint Operations Platform', which uses AI to create lists of 'suspicious people' who then may subject to detainment. Classified Chinese government documents released by the International Consortium of Investigative Journalists (ICIJ) in November 2019 revealed that more than 15,000 Xinjiang residents were placed in detention centres during a seven-day period in June 2017 after being flagged by the algorithm. The detainees seem to have been targeted for a variety of reasons, including traveling to, or contacting people from, any foreign countries China considers sensitive, attending services at mosques, having more than three children, or sending texts containing Quranic verses. The Chinese government called the leaked documents 'pure fabrication' and maintained that the camps are education and training centers. See: UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 'Racial discrimination and emerging digital technologies: a human rights analysis', A/HRC/44/57, 18 June 2020, par. 39. ; Maizland, L., 'China's Repression of Uyghurs in Xinjiang', Council on Foreign Relations, 1 March 2021.; Allen-Ebrahimian B., 'Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm', International Consortium of Investigative Journalists, 24 November 2019.

[35] Ibidem.

[36] Hoffman, S., 'Managing the State: Social Credit, Surveillance and the CCP's Plan for China' in: Wright, N., 'AI, China, Russia, and the Global Order. Technological, Political, Global, and Creative Perspectives', NSI, 2019.

restrictions on movement, education, and financial transactions. By contrast, people and legal entities ranked highly could win tax reductions or privileged access to governmental and private services, including deposit waivers, free library book borrowing, or shorter lines at airport security[37]. During the pandemic, the Chinese government has combined the pre-existing monitoring apparatus and biometric records with invasive new apps and opportunities for data collection to identify potentially infected persons and enforce population quarantine (e.g. by using drones and upgrading facial-recognition cameras with thermal detection technology[38]).

Many other governments besides the Chinese (including in countries across the democratic spectrum) have been rolling out biometric and AI-assisted surveillance with few or no protections for human rights, however. The rise of biometric surveillance, in particular facial recognition technology, can be observed in different parts of the globe, despite evidence that it may exhibit bias and lead to or reinforce discrimination[39], alongside being intrusive in nature, lacking regard for privacy. The countries that have recently been expanding facial recognition cameras in public spaces, for example, include Kyrgyzstan[40], India[41], a number of Latin American countries[42], as well as some 'Global North countries' such as Israel (which has implemented the system on the West Bank)[43], the United States[44], and Australia[45]. The most prominent example of AI-assisted surveillance is Russia, where the pandemic has accelerated a process of installing a network of 100,000 facial recognition cameras to keep track of quarantined individuals[46]. The expansion of this technology has contributed to the regime's already pervasive surveillance mechanisms based on, among others, pre-existing and ever-expanding laws allowing for mass surveillance and curbing of internet freedom[47]. These developments increase the authorities' capability to monitor both online and offline spaces and facilitate targeting of peaceful protesters, cracking down on critical media and repressing civil society organisations. They also enhance the government's capacity to conduct fine grain censorship[48].

The expansion of algorithmic decision-making systems, including those processing biometric data or making inferences about sensitive personal data, extends to a number of different fields, including distribution of public services, social security, healthcare, policing, administration of justice, education, finance, immigration, and commerce. In the criminal justice context, for example, police departments in different parts of the world (e.g. the United States, China, India) have been using emerging digital technologies for predictive policing[49], whereby AI systems pull from multiple sources of data, such as

[37] Freedom House, 'Freedom of the Net 2020. China Country Report', 2020.; Kostka, G., 'China's social credit systems and public opinion: Explaining high levels of approval', New Media & Society, 27(7), 2019.
[38] Roberts, S.L., 'Tracking COVID-19 using big data and big tech: a digital Pandora's Box', LSE British Politics and Policy, 2020.; Ada Lovelace Institute, 'Exit Through The App Store', 2020.
[39] Singer, N. and Metz, C., Many Facial-Recognition Systems Are Biased, Says U.S. Study', The New York Times, 20 December 2019. ; Interview with Jonathan McCully, Legal Adviser, Digital Freedom Fund, 17 December 2020.
[40] Human Rights Watch, Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights, 15 November 2019.
[41] Ulmer, A. and Siddiqui Z., 'India's use of facial recognition tech during protests causes stir', Reuters, 17 February 2020.
[42] Interviews with Juan Carlos Lara, Research and Policy Director, Derechos Digitales, 09 December 2020 and Interview with Gaspar Pisanu, Latin America Policy Manager, Access Now, 6 January 2021.
[43] Ziv, A.,'This Israeli face-recognition start-up is secretly tracking Palestinians', Haaretz, 15 July 2019.
[44] Human Rights Watch, 'Rules for a New Surveillance Reality', 18 November 2019.
[45] Bavas, J., 'Facial recognition system rollout was too rushed, Queensland police report reveals', ABC, 5 May 2019.
[46] BBC, 'Russia: Moscow uses facial recognition to enforce quarantine', 3 April 2020.
[47] Claessen, E., 'Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU', Journal of Cyber Policy, 5(1), 2020.; European Court of Human Rights, 'Zakharov v. Russia', No. 47143/06, 4 December 2015.; Human Rights Watch, 'Russia: Social Media Pressured to Censor Posts', 5 February 2021. See also Figure 5 and 6.
[48] Human Rights Watch, 'Russia', 2020.; Activists A. Popova and politician V. Milov have lodged a complaint over Russia's use of facial recognition technology during protests to the European Court of Human Rights. This will be likely the first case challenging the use of facial recognition technology to conduct mass surveillance in the court's practice.
[49] Automated predictions about who will commit crime, or when and where crime will occur.

criminal records, crime statistics and the demographics of neighbourhoods[50]. Another example may be drawn from the area of social security. The use of digital technologies has contributed to the emergence of a so-called 'digital welfare state' in many countries across the globe, a trend considered to provide 'endless possibilities for taking surveillance and intrusion to new and deeply problematic heights'[51]. This particularly applies to the development of digital identification systems that involve the collection of various forms of biometric data and are used to determine the distribution of social benefits and access to public services (see Box 1). Governments that have been experimenting with incorporating these technologies into their welfare systems include:

- India;
- Kenya;
- South Africa;
- Argentina;
- Bangladesh;
- Chile;
- Jamaica;
- Malaysia;
- the Philippines;
- the United States[52].

All these algorithmic systems raise grave concerns, as the basis for their decision-making is opaque, but opportunities to appeal and get redress in cases of abuse are very limited, if existent at all. There is also a risk that many of the data sets fuelling these systems reflect existing racial or ethnic bias, despite the presumed 'objectivity' of these technologies. It has been established that they can operate in ways that reinforce discrimination and cause serious harm, in particular to people from certain racial or social groups (such as people with non-white faces, or the poor[53]). In the law enforcement sector, errors may lead to false accusations and arrests. In the context of distribution of social welfare, they may result in unjustifiable loss of benefits or reduced access to services, and eventually contribute to reinforcing social inequalities.

**Box 1 : Examples of algorithmic harm**

**Predictive policing**

The 'Correctional Offender Management Profiling for Alternative Sanctions – COMPAS' system is a notorious example of an AI system with discriminatory effects. It is a scoring tool used in some states in the United States (US) to assess the risk of someone committing a crime, with the aim of helping judges to determine whether they should be allowed to go on probation. While the system did not directly consider the racial origin or skin colour of the assessed person, a detailed analysis of the results showed that black people were more often rated as risky in terms of committing a crime than white people[54].

[50] McCarthy, O.J., 'AI & Global Governance: Turning the Tide on Crime with Predictive Policing', United Nations University - Centre for Policy Research, 26 February 2019.
[51] UN Special Rapporteur on extreme poverty and human rights, 'Report A/74/493', 11 October 2019, par. 26.
[52] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, op. cit. par. 41; Special Rapporteur on extreme poverty and human rights, op. cit., par. 20.; Interview with Juan Carlos Lara, Research and Policy Director, Derechos Digitales, 09 December 2020.
[53] Zuiderveen Borgesius, F., Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, p. 12,17. The study discusses risks of discrimination caused by algorithmic decision-making and other types of AI, explaining inter alia, how and in which fields those systems create discriminatory effect.
[54] Zuiderveen Borgesius, F., op. cit. , p. 14.

**Digital identification systems**

The world's two largest digital identification systems are 'Huduma Namba' in Kenya and 'Aadhaar' in India. Among other data, they involve the collection of fingerprints, retina and iris patterns, voice patterns, and other identifiers. They determine access to essential government services (such as voting, registering birth certificates and civil marriages, or paying taxes) or access to pensions and unemployment benefits. However, there is evidence that, 'when trying to access public services through these systems, certain racial and ethnic minority groups in both countries find that they are excluded, while others face logistical barriers (...) that in effect can result in de facto exclusion from services to which they are entitled'[55]. Furthermore, people with disabilities have 'experienced discrimination for not being able to provide fingerprint or iris scans'[56].

## 2.2 Emergence of public health surveillance systems

Apart from the expansion of existing surveillance systems, the COVID-19 crisis has also led to the unveiling of many high-tech tools specifically aimed at tackling the pandemic. The most prominent example is a rapid rollout of pandemic-related mobile applications used for contact tracing, quarantine enforcement, social distancing monitoring, or symptom tracking, sometimes combined with a health status code. Such smartphone apps have been introduced in at least 54 countries across the globe[57]. These technologies may offer benefits to policymakers, the medical community, and to society at large (for example, by supporting efforts to protect public health and manage the crisis), but their widespread application also carries significant implications for fundamental rights. In many instances, these tools have been developed with minimal protection against abuse (such as excessive use by law enforcement agencies for non-pandemic-related purposes), without sufficient evidence to confirm their efficacy to protect public health or appropriate scrutiny into whether they are proportionate to counter-epidemic efforts[58]. Even though the use of mobile location data may reveal sensitive information about people's identity, location, behaviour, associations, and activities, many developers have largely ignored principles of privacy-by-design, which would ensure that privacy considerations are built into a tool's architecture and software. Apps are often closed sourced, centralised (sending unencrypted data to centralised government servers) and with insufficient cyber-security standards, allowing data to be shared with multiple institutions. This is particularly problematic in the case of repressive regimes, where human rights defenders, independent journalists, or opposition leaders are routinely targeted, as apps that generate sensitive health and social networking data about these individuals increase opportunities for abusive surveillance. Moreover, in some countries (Singapore, Ukraine, and Bahrain, for example) apps have been made mandatory, having a disproportionate and discriminatory impact on certain populations, particularly when non-digital alternatives are not provided (see Table 1). In other countries, such as China, India, and Turkey, COVID-related health status and contact-tracing mobile apps, even though not officially mandatory, have been made gatekeepers for access to essential public services, such as public transport and other public spaces, workplaces or shopping malls[59].

[55] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, op. cit. par. 40. UN Special Rapporteur on extreme poverty and human rights, op. cit., par. 15.
[56] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, ibidem.
[57] Freedom House, 'Freedom of the Net 2020 Report', 2020, op. cit., p. 15.
[58] Joint civil society statement, 'States use of digital surveillance technologies to fight pandemic must respect human rights', 2020.
[59] Freedom House, 'Freedom of the Net. 2020 Report', 2020, op. cit., p. 15.

**Table 1: Examples of human rights implications of mandatory pandemic-related apps**

| Country | Type of application | Problem | Explanation |
|---|---|---|---|
| **Singapore** | Contact-tracing app | Discriminatory impact | The app is obligatory for some categories of migrant workers who already faced discrimination, increasing the risk of further marginalisation of this group[60]. |
| **Ukraine** | Quarantine-enforcement app | Discriminatory impact<br>Risk of exposure to life-threatening situations | The government required people crossing its borders to install the app to monitor compliance with self-isolation orders. This has particularly affected elderly people in the Donetsk region, where many are unable to download the app and are therefore denied entry to government-controlled territory, instead left stranded in an active conflict zone[61]. |
| **Bahrain** | Quarantine-enforcement app | Excessive punishment | Individuals failing to comply with the obligation to use the mandatory app and wear the electronic wristband which comes with it face severe criminal sanctions (up to 26,000 USD fine and/or a minimum three-month jail term)[62]. |

Data-driven responses to the pandemic are not limited to mobile apps. In different parts of the world, they also include solutions such as digital permit systems for non-essential travel, both on public transport and in private vehicles (Russia[63]); expansion of state access to data stored by telecommunications companies (in at least 30 countries across the world[64]); and the aggregation of data on new public health platforms from different sources. The last two measures have been deployed in Ecuador, where the government has introduced laws enabling satellite tracking of people suspected of having COVID-19 to ensure that they are complying with isolation requirements, and has also established a platform aggregating location data, surveillance camera footage, and data from a symptom-checking app[65].

Overall, the pandemic has likely led to the emergence of new ways of 'digital social sorting, in which people are identified and assigned to certain categories based on their perceived health status or risk of catching the virus'[66]. It has also exposed the problem of public-private partnerships in the area of surveillance, as many governments have provided their pandemic-related technological solutions in collaboration with private companies that develop surveillance tools or process user data (such as telecom companies or internet service providers). This illustrates a wider trend of 'outsourcing' surveillance by states, often with very little transparency and in cooperation with companies 'hiding' behind confidentiality and trade secret exceptions[67]. When those partnerships are implemented without appropriate safeguards and public

[60] Privacy International, 'Singapore contact tracing app made mandatory for migrant workers', 2020.
[61] Human Rights Watch, 'Ukraine: Trapped in a War Zona for Lacking a Smartphone', 26 June 2020.
[62] The National, 'Coronavirus: Bahrain to use electronic tags for people in quarantine', 5 April 2020.
[63] Rudnitsky, J. and Khrennikov, I., 'Moscow Tightens Lockdown With Digital Permits as Virus Spreads', Bloomberg, 10 April 2020.
[64] Ibid, p. 18.
[65] Human Rights Watch, 'Ecuador: Privacy at Risk with COVID-19 Surveillance', 1 July 2020; Association for Progressive Communications and other NGOs, 'Ecuador: Surveillance technologies implemented to confront COVID-19 must not endanger human rights', 19 March 2020.
[66] Freedom House, 'Freedom of the Net 2020 Report', 2020, op. cit. p. 14.
[67] Privacy International, 'Public-Private surveillance partnerships', 2020.

oversight[68], it increases the risk of extending over governments' capability to exploit citizens' data, and also provides private corporations with more opportunities to monetise it. Furthermore, sudden proliferation of pandemic-related apps may contribute to 'normalisation' of widespread digital surveillance, especially as many opaque systems of information collection and predictive analytics have been implemented under the guise of emergency measures, with very little public scrutiny or debate, limiting public awareness of their potential negative and long-term implications[69].

## 2.3 Digital tools of information control

Government-imposed restrictions on electronic communication, such as network disruptions, the shutting down of internet connectivity, bans on entire social networks and applications, or suspension of telephone services, as well as more targeted censorship (like individual website blocking or filtering specific content), are on the rise globally and continue to be an alarming threat to human rights[70]. While they affect freedom of expression, in particular (just as in the case of widespread surveillance), they also interfere with multiple other rights, such as the right to association and peaceful assembly, public participation, privacy, and non-discrimination. The COVID-19 crisis has highlighted their impact on economic, social and cultural rights, as online access to healthcare, education and other essential services, for many people, has become the only viable option.

Internet shutdowns[71] remain one of the most common tools for digital repression, continuing to be used by many governments in different parts of the world to silence dissenting voices, often during critical events, such as protests and demonstrations, elections, or armed conflicts[72]. Internet shutdowns dominate in developing and/or non-democratic countries, where relevant protective legal provisions are non-existent or limited and rarely acted upon[73]. Overall, at least 213 shutdowns were documented in 2019 in 33 countries (India being the current evident 'leader', with at least 385 shutdowns ordered since 2012[74], followed by Venezuela, Yemen and Iraq[75]). This number stands in stark contrast to 2015, when 'only'

[68] Guidelines ensuring transparency and adequate assessment of the human rights impact of any public-private partnerships specifically during COVID-19 have been developed by civil society actors. See: Access Now, Article 19, Association for Progressive Communications (APC), Chinese Human Rights Defenders, CIVICUS, International Service for Human Rights, Ranking Digital Rights, Safeguard Defenders, 'Joint civil society open letter to the UN on public-private partnerships' , 2020.; Open Government Partnership, 'A Guide to A Guide to Open Government and the Coronavirus: Privacy Protections' , 2020.

[69] Csernatoni, R. 'New states of emergency: normalizing technosurveillance in the time of COVID-19', Global Affairs, 6, 2020.; Interview with Diego Naranjo, Head of policy, European Digital Rights, 08 January 2021.

[70] De Gregorio, G. and Stremlau, N., 'Internet Shutdowns and the Limits of Law', International Journal of Communication, 14(202), 2020.

[71] While there is no academic unanimity on the definition of the term 'internet shutdown' and many sources use it interchangeably with 'network shutdown/disruption' or 'blackout', for the purpose of this study we will use a definition developed by Access Now, one of the main advocacy organizations monitoring this problem across the world, which has defined it as 'an 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'. Access Now, 'Keep It On Report 2019', 2020, p. 2.

[72] In 2019, the most commonly observed causes were protests, military actions (mostly in India), communal violence, political instability, religious holidays or anniversaries, and elections, with an aim to undermine collective reaction to those events; Ibidem, p. 13. Interestingly, the evidence suggests that the 'effectiveness' of shutdowns is questionable at best – i.e. that shutdowns are frequently followed by an escalation in the momentum of pre-existing protest, and that activists and citizens use a combination of strategies to continue mobilising. See: Rydzak, J., Karanja, M. and Opiyo, N., 'Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries', International Journal of Communication, 14(2020), 2020, p. 4281.

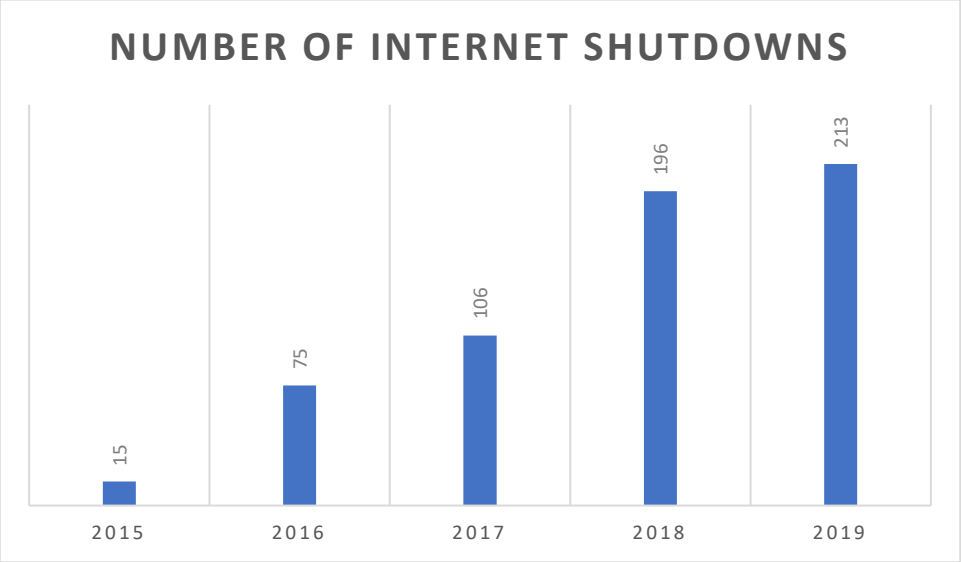
[73] Rydzak, J., 'Disconnected: A human rights-based approach to network shutdowns', Global Network Initiative, 2018, pp. 6-7.

[74] Human Rights Watch, 'End Internet Shutdowns to Manage COVID-19', 31 March 2020.

[75] There is, however, a significant gap between leading India and – next on the list – Venezuela, which was reported to have blocked access to social media platforms at least 12 times in 2019, equal to 86% of internet shutdowns in Latin America (the remaining 14% was attributed to Ecuador). Access Now, op. cit., pp. 2-3.

between 15 and 33 major disruption episodes were registered[76]. Not only have shutdowns been rapidly increasing in number (see Figure 1), but they have also lasted longer and affected more people, especially from vulnerable groups. This is visible, above all, in Africa, where the number of internet shutdowns grew by 47% between 2018 and 2019, and is still on the rise[77]. In Asia, where they are also frequent, shutdowns increasingly target refugees or other minority populations (for example in Myanmar, Bangladesh, India, and Indonesia[78]). Unfortunately, the increasingly severe impact of internet shutdowns on human rights has been additionally exacerbated by the COVID-19 pandemic (see Box 2).

**Figure 1: Number of documented internet shutdowns across the world between 2015 and 2019[79]**




**Box 2: Implications of internet shutdowns in the COVID-19 era**

Internet shutdowns have particularly detrimental effects in light of the COVID-19 crisis. The pandemic has amplified the need for access to reliable, open, secure, and affordable internet.

Intentionally degraded or shut down internet access has impeded effective responses to COVID-19 and threatened people's right to health. It has prevented the dissemination of health information and other crisis-related information, such as updates on government restrictions, which are critical both for the general public and for healthcare workers seeking knowledge and guidelines on treating the virus. Furthermore, blocking people from getting essential services, accessing education and/or work, conducting business, and communicating with families has affected a number of other social, economic, and cultural rights. During periods of isolation, access to all these essential services and opportunities has relied on the Internet even more than usual.

[76] Rydzak, J., op. cit., p. 6.
[77] African country with the biggest number of shutdowns is Algeria (6) followed by Ethiopia (4) and Sudan (3). Giles, C. and Mwai, P. ,'Africa internet: Where and how are governments blocking it?', BBC, 2 November 2020. Shutdowns have been imposed mainly in response to increasing volume of protests and elections-related social unrest; see: Garbe, L., 'What we do (not) know about Internet shutdowns in Africa', 29 September 2020.
[78] Access Now, op. cit., p. 7.
[79] Ibid.; Access Now, 'Keep It On Report 2018', 2019.; Rydzak, J., op. cit. The numbers refer to shutdowns that human rights organisations, such as Access Now, managed to document and verify; the actual number of shutdowns may be higher. For 2015, the available data indicates that there were between 15 and 33 major disruption episodes registered in 2015. See: J. Rydzak, op. cit.

Despite these harmful effects, internet shutdowns have been imposed or continued in at least 14 countries since the crisis began (Bangladesh, Belarus, Ethiopia, India, Indonesia, Iran, Kazakhstan, Myanmar, Pakistan, Philippines, Sudan, Uganda, Zambia and Zimbabwe)[80].

One of the most drastic examples of a shutdown carried out during the pandemic is the internet blackout and phone restrictions imposed by state authorities at the Rohingya refugee camps in Bangladesh, which have been hindering humanitarian groups from addressing the threats posed by COVID-19[81].

It should be noted that shutdowns are not always a monolithic "kill switch", but may vary in scale, scope, location, duration, and frequency. Sometimes restrictions do not involve complete blackouts of internet connectivity across the entire country, but are targeted at a particular region or regions (e.g. recent targeted shutdowns carried out in Ethiopia in the Oromia region[82], or in Myanmar in parts of the Rakhine and Chin states[83]). They may also constitute a more 'subtle' disruption in the form of deliberate slowdowns, often leading to the same practical effects as full shutdowns (e.g. after lifting a seven-month blanket internet shutdown in Jammu and Kashmir in 2020, the Indian authorities have restricted internet access to only slow-speed 2G[84]). Other governments 'focus' on online platform blocks, targeting global platforms with dominant positions on the market, which have become key channels for accessing information, in particular[85] (in Venezuela, for example, access to social media such as Facebook, Twitter, and Instagram was blocked at least 12 times in 2019[86], or most recently during the military coup in Myanmar[87]). Official government justifications for imposing these measures range from a need to combat fake news and hate speech, to public safety and national security. These justifications rarely match what observers conclude to be the actual cause, however[88].

Other forms of restricting the free flow of information online used by governments to censor critical voices involve more targeted access restrictions, such as Internet Protocol ('IP') Address blocking, Domain Name System ('DNS') filtering, and redirection or Uniform Resource Locator ('URL') filtering[89] (e.g. 'the world's most advanced apparatus for such internet censorship' operated by China, known as the 'Great Firewall'[90]). Furthermore, states are putting increasing pressure on tech companies to take down content and share user data, which can be observed in transparency reports published by large online platforms[91]. In 2020,

[80] Freedom House, 'Freedom of the Net 2020 Report', 2020, op. cit., p. 10.; See also the Excel data for the list of countries; Access Now, 'Cutting internet access when people need it the most: stories from Uganda', 9 February 2021.
[81] The shutdown followed several security-related incidents involving camps' residents. See more at: Human Rights Watch, Bangladesh: Internet blackout on Rohingya Refugees, 13 September 2019.; Join letter of several human rights NGOs, 'Restrictions on Communication, Fencing, and COVID-19 in Cox's Bazar District Rohingya Refugee Camps', 2 April 2020.
[82] Access Now, 'Ethiopia: Communications Shutdown Takes Heavy Toll', 9 March 2020.
[83] Access Now, 'Keep It On Report 2019', 2020, op. cit., p. 4.
[84] There have been several reports indicating that residents in Jammu and Kashmir are unable to access information about COVID-19 due to the restriction on high-speed 4G internet access in these areas. It has been also revealed that the restrictions make access to video conferencing – currently a critical lifeline throughout India and much of the world – virtually impossible; Access Now, '#KeepItOn: Open letter appealing to the Deputy Director-General to urge the governments of Bangladesh, India, Myanmar, and Pakistan to end the ongoing internet shutdown amid COVID-19 pandemic', 26 May 2020.
[85] See also Box 4 below for data on how global digital market is dominated by a handful of online platforms.
[86] Access now, 'Keep It On Report 2019', 2020, op. cit., p. 7.
[87] BBC, 'Myanmar coup: Military blocks Facebook for ake of stability', 5 February 2021.
[88] See footnote no. 66.
[89] These are different, IP, DNS or URL-based online content blocking techniques which from the user's perspective lead to the same effect, namely some parts of the internet inaccessible. For more detailed descriptions of these techniques see: Internet Society, 'Internet Society Perspectives on Internet Content Blocking: An Overview', 2017.
[90] Not only blocking access to tens of thousands of sites and domain names, but also enabling automated and systematic internet censorship of content criticising the regime. Garside, S., 'Democracy and Digital Authoritarianism. An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom', College of Europe - EU Diplomacy Papers 1/2020, 2020.
[91] Ranking Digital Rights, 'The RDR Index 2019', 2020.

this trend also involved blocking independent media websites reporting on the spread of COVID-19 to suppress unfavourable health statistics or critical reporting on governments' responses to the crisis. Censorship of COVID-19 content was registered in at least 28 countries, with most prominent examples in China, Venezuela, and Egypt[92].

Other ways that governments enhance their censorship capacity include the introduction of new legislation, a trend that is not new, but again amplified by the pandemic. During the COVID-19 crisis, at least 20 countries adopted new regulations, sometimes as part of state of emergency laws, through which vague and overly broad speech restrictions were imposed[93]. In particular, governments responded with the enactment of laws that criminalised fake news and provided excessive, harsh penalties for those found guilty of spreading it, as well as by imposing new regulations for online platforms (see Table 2).

**Table 2: Examples of new laws challenging internet freedom**

| Country | Main provisions | Sanctions |
|---|---|---|
| **Tanzania**[94] | The new law:<br>• Requires that bloggers and other content providers register and pay expensive licensing fees for publishing content online<br>• Expands the list of prohibited content to include informing about deadly or contagious disease without authorities' permission<br>• Forces online services providers to filter and censor content using automated tools, such as upload filters, and requires immediate takedown of alleged illegal content without due process safeguards | A person who publishes prohibited content shall, upon conviction, be liable to a fine of not less than 2,000 USD and/or imprisonment for no less than 12 months |
| **Zimbabwe**[95] | The new law penalises false information about the pandemic[96] in both online and offline (real life) environments | Fine of up to 10,000 USD and/or imprisonment for a period not exceeding 20 years |
| **Russia**[97]<br><br>Multiple internet-related laws were adopted in | Penalise public dissemination of knowingly false information leading to grave consequences, which caused harm to an individual's health (criminal law) | Among other sanctions, a fine of 19,000 to 25,500 USD, correctional labour, or up to 5 years of imprisonment |
| | Address the dissemination of false or inaccurate information by legal entities that are using mass media or the internet (administrative law) | A fine of up to 127,800 USD and confiscation of equipment |

[92] Freedom House, 'Freedom of the Net 2020 Report', 2020, op. cit. p. 10.
[93] Ibid.
[94] Access Now, 'Internet censorship in Tanzania: the price of free expression online keeps getting higher', 20 October 2020; The Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 'State of internet freedom in Africa. Resetting Digital Rights Amidst The COVID-19 Fallout', 2020, p. 6.
[95] Ibid.
[96] The law penalises precisely publication or communication of false or fake news about 'any public officer, official or enforcement officer involved with enforcing or implementing the national lockdown in his or her capacity as such, or about any private individual that has the effect of prejudicing the State's enforcement of the national lockdown; Ibid.
[97] The Law Library of Congress, 'Freedom of Expression during COVID-19', 2020, p. 44-45.; Human Rights Watch, 2021, op. cit.

| | | |
|---|---|---|
| 2020/2021, which: | Penalise 'libel' committed online (criminal law) | A fine of up to 13,300 USD and/or up to 2 years of imprisonment |
| | Oblige hosting providers to remove content deemed illegal under Russian law (administrative law) | A fine of up to 13,500 USD and, in the event of repeated offense, up to 10% of any company's annual revenue |

Besides that, numerous states continue to take punitive actions against bloggers, journalists, activists, or whistle-blowers publishing on the Internet, often based on spurious charges of spreading hate speech or fake news. This is, again, not a new trend, but remains very present in many parts of the world[98]. In 2020, this trend affected dissemination of credible and timely information about the pandemic in particular, which has been undermined by retaliation against political opponents, journalists, human right lawyers, and healthcare workers engaging in online discourse about COVID-19 (e.g. revealing the actual scale of the outbreak or speaking out about unsafe working conditions in the health sector). Overall, in at least 45 countries, activists, journalists, and other members of the public were arrested or charged with criminal offenses for online expression related to the pandemic, based either on laws passed before the coronavirus crisis, or on new legislation tailor-made for the pandemic[99]. Such criminal investigations have been opened in, among other countries, Russia, Turkey, Venezuela, Tanzania, Morocco, Kenya, and China, where recently one such 'whistle-blower', Zhang Zhan, was sentenced to four years imprisonment[100].

Finally, in a growing number of countries, network disruptions and other repressive actions impeding access to online information have been facilitated by efforts to enhance 'sovereign control' over online information space. Multiple states have adopted measures to control the flow of data in and out of their national borders and isolate 'domestic' internet from the global network. Imposing new restrictions on cross-border data transfer and storage, as well as centralising technical infrastructure, is often justified by the authorities as responsive to the need to protect user privacy and improve cyber-security, particularly in the context of threats posed by globally-operating online platforms. In countries with no due regard to human rights, however, it may as well be used as a tool for extending surveillance and censorship through even more pervasive monitoring and filtering of all traffic coming to the country, as well as easier access to sensitive information and user data for domestic law enforcement agencies. While China and Russia have been the key driving force behind 'cyber sovereignty' (see Box 3), it has recently been expanding particularly quickly in countries such as Iran, Brazil, India, Turkey, Vietnam, and states in North Africa[101]. At the same time, it needs to be flagged that states' efforts to increase national control over global online platforms and, more generally, over the 'domestic internet', albeit motivated by different intentions, have

[98] Still, according to the Reporters Without Borders, more than a half of the world's imprisoned journalists (61%) are being held in just five countries: China, Egypt, Saudi Arabia, Vietnam and Syria. Reporters Without Borders, 'Round -up 2020. Journalists detained, held hostage and missing', 2020.
[99] Freedom House, 'Freedom of the Net 2020 Report', 2020, op. cit. p. 11.
[100] Human Rights Watch, 'Russia: Health Workers Face Retaliation for Speaking Out', 15 June 2020.; Human Rights Watch, 'Turkey: Probes Over Doctors' COVID-19 Comments', 10 June 2020; Human Rights Watch, 'Venezuela: A Police State Lashes Out Amid COVID-19', 28 August 2020. The Collaboration on International ICT Policy for East and Southern Africa (CIPESA), op. cit., p. 9-10.; V. Wang , V., 'Chinese Citizen Journalist Sentenced to 4 Years for COVID Reporting', 28 December 2020.
[101] Shahbaz, A. Funk, A. and Hackl, A., 'User Privacy or Cyber Sovereignty?', Freedom House, 2020.; Gifford, C., 'What a sovereign internet could mean for free speech', The New Economy, 6 August 2019.

become a global trend also present in Western countries, including in the EU's pursuit of strengthening its 'digital sovereignty'[102].

**Box 3: Cyber sovereignty in China and Russia**

**China**

China has long pursued a cyber sovereignty agenda aimed at increasing control over 'national' internet with restrictive internet policies, including in particular the infamous 'Great Firewall'. Among other limitations, those policies prevent citizens from accessing certain foreign information sources (as a result of blocking selected websites and services that the government has put on its blacklist) and force overseas tech companies to adapt to China's domestic regulations. The 2017 Cyber-security Law expanded the cyber sovereignty trend by, among other things, requiring that critical information infrastructure operators store personal and important data domestically and make it accessible on demand to the authorities, introducing 'security assessments' necessary for the transfer of any such data abroad, or imposing the user real-name registration obligation by network operators. In the wider context of crackdown on internet freedom in China, these provisions are believed to further undermine human rights in digital space in the country[103].

**Russia**

In 2019, Russia introduced a package of laws concerning the 'autonomous Russian internet'. The laws foresee that 'internet traffic within Russia could only go through Internet exchange points (IXPs) that are pre-approved by the institution issuing control and supervision of the internet, Roskomnadzor'[104]. In practice, 'this creates a system that gives the authorities the capacity to block access to parts of the Internet in Russia, potentially ranging from cutting access to particular internet service providers through to cutting all access to the Internet throughout Russia'[105]. Such a scenario does not seem unrealistic in light of recently documented internet outages[106] and escalating pressure on online platforms to remove content deemed illegal by the authorities[107], amid protests against the detention of prominent opposition activist Alexei Navalny, and in light of other rapidly growing concerning internet policies in Russia (see Table 2).

## 2.4 Next generation repression toolkit

There are also a number of fairly recent trends encompassing the 'next generation' of techniques used by governments to interrupt citizens' access to online information and target their privacy, which are likely to further expand in the future. Over time, repressive regimes have developed an arsenal that extends from technical measures, laws and policies to more covert and offensive techniques including targeted malware

[102] European Commission, 'Regulation on data governance - Questions and Answers', 2020.; Burrows, M. and Mueller-Kaler J., 'Smart Partnerships amid Great Power Competition: AI, China, and the Global Quest for Digital Sovereignty', Atlantic Council, 202.

[102] Access Now, 'A closer look at China's Cybersecurity Law - cybersecurity, or something else?',13 December 2017.

[102] Claessen, E., op. cit.; Human Rights Watch, ''Joint Statement on Russia's 'Sovereign Internet Bill' by 10 human rights, media and Internet freedom organisations', 24 April 2019.; Netblocks, 'Internet disrupted in Russia amid opposition protests', 23 January 2021.

[103] Access Now, 'A closer look at China's Cybersecurity Law - cybersecurity, or something else?', 13 December 2017.; Claessen, E. (2020), op.cit.; Human Rights Watch, 'Joint Statement on Russia's 'Sovereign Internet Bill' by 10 human rights, media and Internet freedom organisations, 2019, op.cit.

[104] Claessen, E. (2020), op.cit.;

[105] 'Joint Statement on Russia's 'Sovereign Internet Bill' by 10 human rights, media and Internet freedom organisations, 24 April 2019, www.hrw.org/news/2019/04/24/joint-statement-russias-sovereign-internet-bill.

[106] Netblocks (2021), 'Internet disrupted in Russia amid opposition protests', 23 January.

[107] One of the new laws adopted in January 2021 was already used to impose fines on a number of online platforms which were considered not to have complied with an obligation to remove illegal content related to 'incitement to participate in the unlawful protests'. See, Roskomnadzor (2021), 'Социальные сети будут привлечены к ответственности за вовлечение подростков в противоправную деятельность', 27 January. Human Rights Watch (2021), 'Russia: Social Media Pressured to Censor Posts' (…), op. cit.

attacks, such as Distributed Denial of Service attacks (DDoS attacks[108]) or targeted cyberespionage campaigns[109]. The use of such techniques was documented in most countries which, according to Freedom House's latest 'Freedom on the Net' report, have the worst conditions for internet freedom, or have experience the biggest decline in internet freedom recently. These include, among others:

- China, using malware redirecting the website requests of unwitting foreign users into DDoS attacks or replacing web requests with malicious software[110];
- Kyrgyzstan, where independent media websites were disabled by DDoS attacks;
- India, using spyware against prominent activists, journalists, and lawyers involved in advocating for the rights of marginalised groups;
- Nigeria, with cyberattacks targeted at independent journalists and media outlets;
- Rwanda, where spyware was used to monitor and intimidate exiled dissidents[111].

Sophisticated spyware attacks on human rights defenders, activists and journalists are increasingly backed up by states' efforts to undermine the technology which provides these groups with important means to protect their security online and, in general, facilitates the exercise of human rights in a digital age. Repressive regimes respond to its use by blocking secure messaging apps, implementing so-called 'back-door access' in commercially available products, or introducing laws compromising user anonymity, such as limits on virtual private networks ('VPN'), encryption or imposing real-name registration obligations[112].

The next generation techniques also involve efforts to indirectly impede the free flow of information by engaging government-recruited 'troll armies' that, looking like spontaneous expression, use privately-owned popular online platforms to discredit or intimidate any dissenting voices or disseminate disinformation aimed at drowning out accurate content. Apart from a negative impact on the right to privacy of those targeted by such actions, their ultimate goal is often to generate a 'chilling effect' on freedom of expression – i.e. to discourage activists or independent journalists from using digital communication for fear that they would be monitored or intimidated. Examples of pro-government 'e-warriors' include India's 'Modi's Yoddhas', associated with the ruling Hindu nationalist Bharatiya Janata Party, Russia's 'Kremlin's troll army', the Brazilian 'President Bolsonaro's hate office' or the Vietnamese 'Force 47'[113].

While attacks on the internet target different categories of victims, one of the continuing challenges, which has been receiving increasing attention from researchers and human rights organisations in recent years

[108] 'A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. (...) A distributed denial-of-service (DDoS) attack occurs when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.' See: CISA (2019), 'Understanding Denial-of-Service Attacks', November 20.

[109] Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott—Railton, J., Deibert, R. and Paxson, V., 'China's Great Cannon', Citizen Lab, University of Toronto, 10 April 2015.

[110] Deibert, R., 'Authoritarianism Goes Global: Cyberspace Under Siege', Journal of Democracy, 26 (3), 2015.

[111] Freedom House, 'Freedom of the Net 2020 Report', 2020, op. cit., p. 6.

[112] The most prominent examples of countries where such measures have been adopted over the recent years are China and Russia. See, Freedom House, 'Freedom of the Net 2020. China Country Report 2020', 2020.; Human Rights Watch, 'Russia: New Law Expands Government Control Online', 31 October 2019.

[113] Reporters Without Borders, 'RSF unveils 20/2020 list of press freedom's digital predators', 10 March 2020.

has been continuing gender-based harassment, including cyber violence faced by women. Not only do women appear to be disproportionately targeted, but attacks against them often also involve particular forms of online abuse, including sexuality-related threats (such as stalking, rape threats, doxing, and non-consensual disclosure of sexually explicit images and videos). Such harassment targets, in particular, female journalists, human rights defenders who speak out against government abuses and on women's rights issues, politicians and opposition leaders, and other women engaging in public debate, intimidating them out of the public space and spurring discrimination[114].

Another emerging challenge for a free flow of information online, which will likely become more ubiquitous in the future is the rise of automated censorship. This often encompasses sophisticated content filtering techniques that engage algorithms powered by machine learning and, in some parts of the world (in China, for example) already fuelling real-time censorship tools without explicit user notice (which makes it 'more difficult to detect and react to because it is being done invisibly upstream of the user')[115]. In a number of countries (in India[116], for example, or already-mentioned Tanzania) new legislation has been adopted recently obliging service providers to proactively filter online content, without sufficient safeguards preventing the possible abusive use of such tools.

At the same time, automation in content moderation has increasingly been used on a voluntary basis by the most popular global online platforms. Even when not applied with intent to silence any particular voices, it in fact 'exposes all speech to a form of evaluation *ex ante* and in a way that fails to consider linguistic, social, historical, and other relevant context'[117]. It creates substantial risks to freedom of expression, especially when coupled with a lack of due process safeguards available to users, including transparency and effective remedies. The is exacerbated by the lack of independent, external oversight of platforms' decisions and the fact that these actors, not only due to specificities of their services but also their dominant positions on the market, serve as powerful gatekeepers for public discourse and access to information (see Box 4). One of the most disturbing recent examples of such 'privatised censorship' carried by large tech companies concerns suppressing dissenting voices from marginalised and oppressed communities on platforms such as Facebook and Twitter in the Middle East and North Africa (MENA) region. They include arbitrary and non-transparent suspension and removal of accounts belonging to journalists and activists in Tunisia, Egypt, and Syria (some of which documented war crimes and human rights violations). The scale and frequency of these suspensions suggests that the problem likely results from algorithmic bias, rather than from isolated errors in content moderation[118]. It is also significant that certain regions where big tech companies have not invested sufficiently in localisation or staffing, and where public outcry by digital rights organisations is less likely to trigger platforms' response than in the United States or Europe, may be more vulnerable to the risks of automated censorship. Consequently, users

[114] There are numerous studies that demonstrate prevalence of online harassment and abuse faced by women. See: Article 19, 'Investigating online harassment and abuse of women journalists', 2020; Amnesty International, 'Amnesty reveals alarming impact of online abuse against women', 2017.; Rheault, L., Rayment, E., Musulan, A., 'Politicians in the line of fire: Incivility and the treatment of women on social media', Research & Polictics, 6(1), 2019.; Smętek, J. and Warso, Z., 'Cyberprzemoc wobec kobiet', ('Cyberviolence against woman') (in Polish), Helsinki Foundation for Human Rights, 2017.

[115] Internet Society, 'Policy Brief: Internet Shutdowns', 2019; Ruan, L., Knockel, J., NG, J. Q., Crete-Hishihata, M., 'One App, Two Systems How WeChat uses one censorship policy in China and another internationally', Citizen Lab, University of Toronto, 30 November 2016.

[116] Indian Ministry of Electronics and Information Technology, 'The Information Technology [Intermediaries Guidelines (Amendment) Rules', 24 December 2018.

[117] Llanso, E., van Hoboken, J., Leerssen, P. and Harambam, J., 'Artificial Intelligence, Content Moderation, and Freedom of Expression', Transatlantic Working Group, 2020, p. 25.

[118] Access Now, 'Rights groups to Facebook on Tunisia's "disappeared" accounts: we're still waiting for answers', 23 June 2020; Eskandar, W., 'How Twitter is gagging Arabic users and acting as morality police', Open Democracy, 23 October 2019; Human Rights Watch, 'Video Unavailable. Social Media Platforms Remove Evidence of War Crimes', 10 September 2020.

in smaller or less powerful countries may not receive the same protection against big tech's decisions undermining their fundamental rights as their more influential counterparts[119].

**Box 4: Digital dominance of the largest online platforms in numbers**

According to the UN's Digital Economy Report 2019[120]:

- 40% of the world's 20 largest companies (in terms of market capitalisation) have a platform-based business model;
- Global digital wealth is concentrated in the hands of a few online platforms based in the US and China**.** Both countries account for up to 90% of the market capitalisation value of the 70 largest digital platform companies in the world (US – 68%, China – 22%);
- Europe's share is c.a. 4% and Africa and Latin America's together is only c.a. 1%;
- 7 'super platforms' – Microsoft, Apple, Amazon, Google and Facebook in the US, and Tencent and Alibaba in China – represent 2/3 of the total market value of the 70 largest platforms;
- Some digital platforms have grown to dominate key niches. Google has some 90% of the global market for internet searches, while Facebook accounts for 2/3 of the global social media market and is the top social media platform in more than 90% of the world's economies. Amazon holds 1/3 market share of the world's online retail activity and cloud services.
- In China, WeChat (owned by Tencent) has more than 1 billion active users. Its payment solution and Alipay (owned by Alibaba) have captured virtually 100% of the Chinese market for mobile payments. Meanwhile, Alibaba is estimated to have close to 60% of the Chinese e-commerce market.
- These companies keep consolidating their competitive positions, including by acquiring potential competitors and expanding into complementary products or services, lobbying in domestic and international policymaking circles, and establishing strategic partnerships with leading multinationals in traditional sectors, such as the automotive, semiconductor and retail industries.

Platforms' arbitrariness and lack of transparency in content governance are also routinely used by actors seeking to spread harmful expression, such as racist speech, incitement to discrimination, or violence. Online platforms do not always adequately respond to this threat, as shown, for example, by the role that Facebook played in exacerbating violence against Muslims and the Rohingya ethnic minority in Myanmar in 2017–2018[121]. In addition, online abuse of many marginalised groups is facilitated by social media companies allowing users to cover these actions behind automated accounts. It is also fuelled by their use of data-harvesting and profit-oriented business models, which amplify toxic content[122].

The 'next generation' measures which are used to curb free flow of online information presented in this section may seem more 'subtle' and limited in scope than, for example, blunt-force tactics such as shutdowns. However, what distinguishes them from 'older generation' tools is that they are often less detectable by outside parties and more difficult to assign responsibility for, a feature which likely makes them more effective[123].

[119] Freedom House, 'Freedom of the Net 2020 Report', 2020, op. cit., p. 4; Access Now, Ibid.
[120] United Nations Conference on Trade and Development (UNCTD), 'Digital Economy Report 2019', 2019.
[121] UN Human Rights Council, 'Report of the independent international fact-finding mission on Myanmar', A/HRC/39/64, 2018.
[122] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, op. cit., par. 24-25.
[123] Deibert, R., op. cit., p. 65.

## 2.5 Transnational dimensions of digital repression

Another very serious challenge, which has emerged in recent years, is proliferation of a so-called 'transnational digital repression'[124]. It has become apparent that regimes with restrictive domestic internet policies and advanced digital surveillance have been increasingly 'extending' these practices beyond their borders to affect targets living in foreign countries. In particular, development of new information and communication technologies has facilitated targeting regime opponents living in the diaspora[125]. Even though transnational repression has been a long-standing problem for diasporas with ties to authoritarian sending-states, digital tools have allowed such governments to control, silence, and punish dissent across borders with greater scope, speed and at reduced cost, transcending traditional barriers, such as territorial jurisdiction and physical distance. The rise of new digital and information technologies, services and tools, as well as playing a central role in the targeting of activists based abroad[126], has enabled more effective identification and tracking of dissident networks, including monitoring of their activities, hacking of their social media accounts and websites, the planting of malware, phishing for confidential information, online harassment, and disinformation campaigns. Not only has this facilitated long distance forms of repression targeted directly at those residing abroad, but also 'coercion-by-proxy' – exerting control and inducing fear via relatives still in the country. This is because new methods of digital surveillance make it easier for authoritarian states to identify ties between activists living in diaspora and family members or acquaintances 'back home'[127]. It has also been established that, in response to activists' attempts to protect themselves using methods like encryption, the authoritarian regimes have been applying even more aggressive measures of targeted surveillance (in addition to still in place 'traditional' mechanisms of repression, such as arrests or physical harassment)[128].

The most prominent examples of digital transnational repression are the deployment of cyberespionage campaigns by China against Tibetan diaspora or pro-democracy groups in Hong Kong[129], Saudi Arabia's deployment of spyware on the mobile devices of Saudi political activists living in Canada or the United Kingdom[130], and disruption operations of media and opposition websites based abroad, including defacement and DDoS campaigns by hackers affiliated with Syrian or Iranian regimes[131]. Digital transnational repression practices have also affected targets living in EU countries. It was revealed, for example, that Turkey, known for its current widespread repressive campaign against suspected opponents abroad (including, in particular, mobility controls, detentions and illegal renditions), developed a

[124] Defined as activities undertaken by states 'seeking to exert pressure - using digital tools - on citizens living abroad in order to constrain, limit, or eliminate political or social action that threatens regime stability or social and cultural norms within the country'. See: Al-Jizawi, N., Anstis, S., Chan, S., Senft, A. and Deibert, R. J., 'Annotated Bibliography. Transnational Digital Repression', Citizen Lab, University of Toronto, 2020.

[125] Dalmasso, E., Del Sordi, A., Glasius, M., Hirt, N., Michaelsen, M., Mohammad, A. S., and Moss, D., 'Intervention: Extraterritorial Authoritarian Power', Political Geography, 2017.; Michaelsen, M., 'The Digital Transnational Repression Toolkit, and Its Silencing Effects', Freedom House, 2020.

[126] It has been established that 'for diaspora activists engaging for political change in their country of origin, digital technologies are key to communicate with contacts at home, maintain professional relations, and advocate against rights violations'. This activity makes them particularly 'exposed to monitoring and surveillance from regime authorities'. See Michaelsen, M., ibidem.

[127] Adamson, F.B. and Gerasimos, T., 'At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression', Freedom House, 2020.

[128] Michaelsen, M., op. cit.

[129] Kleemola, K., Crete-Nishihata, M. and Scott-Railton, J., 'Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114', Citizen Lab, University of Toronto, 15 June 2015.

[130] UN High Commissioner for Human Rights, UN experts call for investigation into allegations that Saudi Crown Prince involved in hacking of Jeff Bezos' phone, 22 January 2020; Marczak, B., Scott-Railton, J., Senft, A., Abdul Razzak, B. and Deibert, R.,'The Kingdom Came to Canada. How Saudi-Linked Digital Espionage Reached Canadian Soil', Citizen Lab, University of Toronto, 1 October 2018.

[131] Al-Jizawi, N., et. al, op. cit.

smartphone application to be used for reporting potential members of the Gülen movement[132] to the authorities in Ankara from among the Turkish diaspora in Germany[133]. At the same time, digital threats against activists living abroad have been linked to several other countries across the world in recent years (one of the studies indicates, for example, that the Bahrain, Burma, Eritrea, Ethiopia, Kazakhstan, Rwanda, United Arab Emirates, Uzbekistan, and Vietnam governments are among those implicit in this)[134]. Documented negative effects of such transnational repressive actions on diaspora activism include increased self-censorship among human rights defenders that may be targeted by those practices, more careful management (or even breaking up) of their ties to the home country and higher risk of mental stress and burnout. Still, further research is required to understand how transnational digital repressions affect social and political lives of their target groups[135].

Other examples illustrating an expansion of regime control outside of the nation state, not necessarily targeted at political exiles and diaspora communities, include using the private sector for this purpose. One tactic is to exploit domestic companies functioning on international markets and their technological products to export existing surveillance and censorship practices abroad. There is evidence, for example, that communications on Chinese WeChat, the most popular social media platform in China and third in the world, conducted entirely between non-China-registered accounts, have been 'subject to pervasive content surveillance that was previously thought to be exclusively reserved for China-registered accounts'[136]. Another strategy engaging the private sector involves imposing pressure on globalised tech companies to comply with governments' regulations and suppress the flow of unwelcome information beyond national borders (which, to some extent, may also be facilitated by non-transparent content moderation policies and practices of online platforms[137]). Zoom Video Communications, for example, a US-based video-tech company, recently admitted that, following the Chinese government's demands, it suspended a number of user accounts and ended meetings on its platform linked to the anniversary of China's Tiananmen Square crackdown[138].

Last but not least, digital surveillance in a number of abusive regimes is facilitated by the import of surveillance equipment from other countries, often marketed as tools to assist governments in lawful investigations into crime and terrorism. While certain regimes rely on their own digital surveillance tools, other states (which often do not have the same capacity to develop their own technology), invest in 'off-the-shelf' solutions that are acquired from private sector companies specialising in targeted cyber-espionage. Some of these are based in western countries (including EU Member States), such as the United States, the United Kingdom, Germany, Netherlands, France, Sweden and Israel[139], and have significantly proliferated globally in the recent years. At the same time, China's role in the export of surveillance technologies has significantly increased, offering more affordable packages potentially attractive to

[132] A movement related to a religious leader Fethullah Gülen, which the Turkich government blames for the coup attempt in 2016.
[133] Öztürk, A. E. and Taş, H., 'The Repertoire of Extraterritorial Repression: Diasporas and Home States', Migration Letters, 17(1), 2020, 63-64.; Schenkkan, N. and Linzer, I., 'Out of Sight, Not Out of Reach. The Global Scale and Scope of Transnational Repression', Freedom House, 2021, pp. 38-41.
[134] Al-Jizawi, N., et. al, op. cit.
[135] Michaelsen, M., op. cit.
[136] Knockel, J., Parsons, C., Ruan, L., Xiong, R., Crandall, J. and Deibert, R., 'We Chat, They Watch: How International Users Unwittingly Build Up WeChat's Chinese Censorship Apparatus', Citizen Lab, University of Toronto, 7 May 2020.
[137] Governments may take advantage of those opaque mechanisms to restrict access to politically inconvenient content. Instead of following the required procedures (e.g. getting a court order), they can 'choose the easy way' and use the self-regulation mechanisms of the online platforms to achieve the same result without the procedural restrictions.
[138] Harwell, D. and Nakashima, E., 'Federal prosecutors accuse Zoom executive of working with Chinese government to surveil users and suppress video calls', Washington Post, 19 December 2020.
[139] Reporters Without Borders (2020), 'RSF unveils 20/2020 list of press freedom's digital predators', op. cit.

governments that want to develop their surveillance model[140], while still importing sophisticated biometric surveillance tools from Europe[141].

**Box 5: Pegasus - A global espionage tool?**

A prominent example of a company exporting its spyware products to a number of countries with dubious human rights records is the Israel-based NSO Group. As documented by different human rights organisations, NSO Group's Pegasus mobile phone spyware has been repeatedly misused to target human rights defenders, journalists, lawyers or opposition politicians in at least 4 countries (Morocco, Saudi Arabia, Mexico and the United Arab Emirates), while in general it has been established that the malware was used in 45 states across the globe (including EU Member States such as Greece, France, Latvia, Poland and the Netherlands)[142]. When Pegasus is installed, an attacker has access to a phone's messages, e-mails, media, microphone, camera, calls, and contacts. The attacks are difficult for a victim to detect as they leave few traces and are therefore often carried out leaving little chance to identify perpetrators and hold them to account. In 2019, the NSO Group publicly committed to abide by the UN Guiding Principles on Business and Human Rights. However, an investigation by Amnesty International revealed that just days after the company made that commitment, journalist Omar Radi in Morocco was targeted with NSO's Pegasus software[143].

## 2.6 Conclusions

Even though the proliferation of digital technologies has undoubtedly facilitated the exercise of human rights in many ways[144], the overview of the trends presented in this chapter shows that it has also significantly expanded states' toolkit for repression and social control. These technologies are actively deployed and shaped by many repressive regimes to their own strategic advantage. While China emerges as undisputed leader the in this respect, harnessing sophisticated technologies to undermine human rights has occurred in all parts of the world. This includes both authoritarian and non-authoritarian regimes with advanced technological capacities, as well as less technologically developed states for which opportunities to import 'off-the-shelf' solutions from abroad have become increasingly available.

The main global trend emerging in recent years has been the expansion of sophisticated and ubiquitous data collection, especially a rise of biometric surveillance coupled with algorithmic decision-making (and concomitant challenges posed by algorithmic systems, such as the amplification of existing biases and a lack of transparency in 'black box' machine learning systems). Such mass-scale data collection, conducted in online and increasingly also offline spaces and used for monitoring, assessing, predicting and influencing people's behaviour, has enabled a new mode of governance premised on profiling, sorting,

[140] According to report of the Carnegie Endowment for International Peace, China is already a leader in supplying surveillance technology worldwide (technology linked to Chinese companies—particularly Huawei, Hikvision, Dahua, and ZTE—supply AI surveillance technology in 63 countries, while Chinese product pitches are often accompanied by soft loans to encourage governments to purchase their equipment). One of the most recent examples is the agreement between Kyrgyz government and the China National Electronic Import and Export Corporation to install facial recognition technology in Kyrgyzstan. See, Feldstein, S., 'The Global Expansion of AI Surveillance', Carnegie Endowment for International Peace, 2019.; Human Rights Watch, 'Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights', 15 November 2019.; Human Rights Watch, 'China's Global Threat to Human Rights', 2020. Import of the surveillance equipment from China has also been increasingly prevalent in Latin America. See, Interview with Gaspar Pisanu, Latin America Policy Manager, Access Now, 6 January 2021. One example is the 'intelligent CCTV system' functioning in Ecuador. See: Mozur, P., Kessel, J. M. and Chan M., 'Made in China, Exported to the World: The Surveillance State', New York Times, 24 April 2020.

[141] Dragu, T. and Lupu, Y., op. cit., pp. 32-33; Amnesty International (2020), EU companies selling surveillance tools to China's human rights abusers, 21 September 2020.

[142] Amnesty International, 'Israel: Stop NSO Group exporting spyware to human rights abusers',14 January 2020; Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A. and Deibert, R., 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', Citizen Lab Research Report No. 113, University of Toronto, 18 September 2018.

[143] Amnesty International, 'NSO Group spyware used against Moroccan journalist days after company pledged to respect human rights', 22 June 2020.

[144] Even though this chapter and the whole study focus on threats posed by digital technologies to human rights, some advantageous uses of those technologies have been also flagged (such as encryption tools enhancing privacy and security online or communication technologies facilitating documenting and informing about human rights violations).

and categorising populations. Besides this, more targeted tools for repression and social control are still widely used, including both technological, legal and extra-legal measures, a progressive share of which are 'next generation toolkit' tactics, which encompass practices that are more difficult to detect and hold people accountable for (compared to more 'traditional', blunt-force tactics). These tools and methods are increasingly being 'exported' beyond national borders in various ways, often by states, expanding their 'cyber sovereignty'. This can be observed as another trend that facilitates further restrictions on the free flow of information online, which has become particularly detrimental in the context of the COVID-19 pandemic.

Notwithstanding the omnipresent character of widespread surveillance systems, which affect whole populations on a constant basis, the risk of use of new technologies for repression or control increases, in particular, in times of political tension, protests, demonstrations, armed conflicts and elections. Among the groups most often targeted are human rights defenders and other civil society activists, independent journalists, political opposition, and racial, ethnic and sexual minorities (including women, who are disproportionally affected and face specific types of cyber harassment). In 2020, this list could be expanded to also include healthcare workers who have been whistleblowing about the pandemic. However, when it comes to the proliferation of new technologies, such as digital identity systems, and the emergence of so-called 'digital welfare state', those that are increasingly the most threatened by the abuse of these tools include the poorest, migrants, and other most disadvantaged groups in society.

While the human rights situation in the context of new technologies has been gradually deteriorating over the past two decades, this process has been accelerated by the COVID-19 crisis. Surveillance-led responses to the pandemic have certainly brought the control powers of many states to a new level. They are, however, nothing but an extension of wider mega-trends that have emerged in recent years. These include, first of all, exploiting the state of emergency to justify an increase in long-term restrictions on fundamental rights. Just as in the case of many counter-terrorism measures adopted after the 9/11 attacks, there is fear that new surveillance regimes, introduced in response to the current health crisis, will eventually outlast the pandemic, and, after repurposing, become permanent solutions. Secondly, there is a risk of 'technological solutionism', wherein technology is seen as the only viable option to resolve any social issue, often without appropriate fit-for-purpose and proportionality assessments[145]. Finally, 'surveillance capitalism'[146] facilitates invasive harvesting and exploitation of personal data for profit by private actors, while also allowing state authorities access to these resources. In this context, it is symptomatic that 'responses to COVID-19 have been largely based on the extraction of personal data stemming from public-private partnerships'[147]. This illustrates another phenomenon of the digital era – an essential role of the private sector, which has been highlighted several times throughout this chapter. This includes companies developing and selling surveillance technologies and, in particular, a handful of big tech companies providing globally operating online platforms[148]. These companies exercise concentrated power over billions of people's online expression, access to information and personal data, thanks to which, in many instances, they have become the gatekeepers of fundamental rights in the digital realm.

[145] See e.g., Kitchin, R., 'Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19', Space and Polity Journal, June 2020; Stanley, J. and Granick, J. S., 'The limits of location tracking in an epidemic', American Civil Liberties Union, 2020.
[146] Zuboff, S., 'The age of surveillance capitalism: The fight for a human future at the new frontier of power', New York: Public Affairs, 2019.
[147] Mitsilegas, V., 'Responding to Covid-19. Surveillance, Trust and the Rule of Law', 2020
[148] Among digital platforms, seven 'super platforms' – Microsoft, Apple, Amazon, Google, Facebook, Tencent and Alibaba – account for two thirds of the total market value of the world's 70 largest platforms. See box above.

# 3 Overview of the international human rights framework

## 3.1 Introduction

This chapter presents an overview of recent developments in the human rights legal framework responding to current trends in the use of new technologies for repression and social control[149]. It will highlight a selection of the most important international laws, standards and other initiatives developed by intergovernmental bodies, both at the international and regional levels, such as the United Nations (UN), Council of Europe (CoE), the Organisation for Security and Cooperation in Europe (OSCE), the Organization of American States (OSCE), and the African Union (AU). It will assess the status of norm development in this area and will identify key gaps that should be confronted by human rights institutions in their future activities.

Legal instruments will be analysed in four categories pertaining to:

1) AI and algorithmic decision-making systems
2) modern surveillance
3) disruptions to free flow of information on the internet,
4) human rights responsibilities of private actors.

It has been widely recognised that human rights apply to the internet and other digital technologies. In 2012, the UN Human Rights Council adopted a 'Resolution on the promotion, protection and enjoyment of human rights on the Internet'[150], for example, affirming that 'the same rights that people have offline must also be protected online; in particular, freedom of expression, which is applicable regardless of frontiers and through any media of one's choice'. The main general international human rights instruments, therefore, including binding treaties such as the International Covenant on Civil and Political Rights ('ICCPR') or the European Convention of Human Rights ('ECHR') (see Box 6), while not specific to new and emerging technologies, in principle may be invoked to address the current human rights challenges posed by these technologies. This also applies to the key instruments protecting social, economic, and cultural rights (see Box 6) which, as already flagged in the previous chapter, are increasingly relevant in this context. It thus follows that design, development and deployment of any digital technologies are subject to the international human rights law three-part test, which requires that any measures restricting those rights must meet criterion of legality, pursue a legitimate aim, as well as be necessary and proportionate to achieve this aim[151]. This means, in particular, that the use of digital technologies interfering with human rights must be always the exception, rather than the rule, must be provided in law, applied only in specific circumstances, and involve the least restrictive means possible.

At the same time, due to generic nature of the human rights treaties, in order to sufficiently meet emerging challenges pertaining to the use of new technologies and ensure their adherence to human rights standards, there is a need for more detailed guidelines. These guidelines can often be found in the 'soft law' instruments developed within different human rights institutions. Even though they do not have a binding force, they play an important role in interpreting and applying international norms, and may induce compliance with them by state and non-state actors. Moreover they have the potential to respond

[149] As also indicated in the Note on methodology, the analysis will be focused mainly on instruments adopted in the course of last 5 years.
[150] UN Human Rights Council, Resolution on 'the promotion, protection and enjoyment of human rights on the Internet', A/HRC/20/L.13, 2012. The resolution started a series of subsequent resolutions with the same title adopted over the previous decade which have been progressing and consolidating its standards. There have been four resolutions adopted to date, the most recent one in 2018.
[151] See for example Articles 8-11 of the ECHR.

to the most actual problems, which – given the very dynamic nature of the field in question – is a significant asset of these documents. In light of a limited number of binding instruments specifically addressing repression and social control facilitated by the use of new and emerging technologies, the following chapter will thus focus to a great extent on the analysis of available soft law instruments. The analysis of this legal framework will be complemented by highlighting selected standards provided recently in the jurisprudence of the international courts.

**Box 6: Main human rights international treaties and rights most affected by the use of digital technologies for repression and social control**

**United Nations:**

- **International Covenant on Civil and Political Rights ('ICCPR')**[152]

  Article 2 (3) – right to an effective remedy
  Article 8 – right to work
  Article 14 – right to a fair trial
  Article 17 – right to privacy
  Article 19 – freedom of expression
  Article 21 – freedom of assembly
  Article 22 – freedom of association
  Article 25 – right to public participation
  Article 26 – non-discrimination

- **International Covenant on Economic Social and Cultural Rights ('ICESCR')**[153]

  Article 2 (2) – non-discrimination
  Article 6 – right to work
  Article 9 – right to social security
  Article 12 – right to the highest attainable standard of health
  Article 13 – right to education
  Article 15 (1) (b) – right of everyone to enjoy the benefits of scientific progress and its applications

**Council of Europe:**

- **European Convention of Human Rights ('ECHR')**[154]

  Article 5 – right to liberty and security
  Article 6 – right to a fair trial
  Article 8 – right to respect for private and family life
  Article 10 – freedom of expression
  Article 11 – freedom of assembly and association
  Article 13 – right to an effective remedy
  Article 14 – non-discrimination

- **European Social Charter ('ESC')**[155]

  Article 1 – right to work
  Article 5 – right to organise
  Article 11 – right to protection of health
  Article 12 – right to social security
  Article 14 – right to benefit from social welfare services
  Article 19 – right of migrant workers and their families to protection and assistance
  Article 20, Article E – non-discrimination

[152] UN, 'Chart of signatures and ratifications of the International Covenant on Civil and Political Rights ('ICCPR')'.
[153] UN, 'Chart of signatures and ratifications of the International of the Covenant on Economic Social and Cultural Rights ('ICESCR')'.
[154] Council of Europe, 'Chart of signatures and ratifications of the European Convention of Human Rights ('ECHR')'.
[155] Council of Europe, 'Chart of signatures and ratifications of the European Social Charter ('ESC')'.

**Organisation of American States:**

- **American Convention on Human Rights ('ACHR')**[156]

  Article 8 – right to a fair trial
  Article 11 – right to privacy
  Article 13 – freedom of thought and expression
  Article 14 – right of reply
  Article 15 – right of assembly
  Article 16 – freedom of association
  Article 23 – right to participate in government
  Article 24 – right to equal protection
  Article 25 – right to judicial protection

- **Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights "Protocol of San Salvador"**[157]

  Article 3 – non-discrimination
  Article 6 – right to work
  Article 8 – trade union rights
  Article 9 – right to social security
  Article 10 – right to health
  Article 13 – right to education
  Article 14 – right to the benefits of culture

**African Union:**

- **African Charter on Human and Peoples' Rights ('AChHPR')**[158]

  Article 2 – right to freedom from discrimination
  Article 7 – right to fair trial
  Article 9 – right to receive information and free expression
  Article 10 – right to freedom of association
  Article 11 – right to freedom of assembly
  Article 13 – right to participate in government
  Article 15 – right to work
  Article 16 – right to health
  Article 17 – right to education
  Article 18 – protection of the family and vulnerable groups
  Article 19 – right of all peoples to equality and rights
  Article 20 – right to self-determination

## 3.2 AI and algorithmic decision-making systems

The development of AI has rapidly expanded over the last two decades. Alongside the increasingly sophisticated use of this technology, including as a tool enabling repressions and social control, setting appropriate standards for it has made it to the top of the agendas of several human rights organisations in recent years. The most comprehensive work has been done within the UN and CoE, while other regional organisations, such as the OSCE, have focused on more specific AI applications.

On the international level, a response to the growing prevalence of AI has been an essential element of the UN Secretary General's efforts to strengthen international cooperation in the field of digital technologies.

[156] Organisation of American States, 'Chart of signatures and ratifications of the American Convention on Human Rights ('ACHR')'.
[157] Organisation of American States, 'Chart of signatures and ratifications of the Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights "Protocol of San Salvador"'.
[158] African Union, 'Chart of signatures and ratifications of the African Charter on Human and Peoples' Rights ('AChHPR')'.

In 2018, the Secretary General released a strategy[159] in which it seeks to align the use of AI with international human rights law in order to define how the UN system will support the use of this technology 'to accelerate achievement of the 2030 Sustainable Development Agenda'. Additionally, the Secretary General has established the High-level Panel on Digital Cooperation (HLPDC). The aim of the HLPDC is to strengthen international and multi-stakeholder cooperation to contribute to the public debate on how to 'optimise the use of digital technologies and mitigate the risks'[160]. Based on the HLPDC 2019 landmark report[161], the Secretary General launched the 'Roadmap for Digital Cooperation'[162]. The Roadmap contains recommendations for concrete actions by diverse stakeholders in eight key areas, including 'supporting global cooperation on artificial intelligence that is trustworthy, human-rights based, safe and sustainable, and promotes peace'. The Roadmap specifically provides potential mechanisms for cooperation, including the establishment of an advisory body on global artificial intelligence, as well as the appointment of a new 'Tech Envoy' in 2021.

At the same time, challenges related to the impact of AI technology have been increasingly addressed by UN human rights mechanisms, such as the Human Rights Council, General Assembly, and Special Rapporteurs, calling both States and business enterprises to ensure the protection of human rights when designing, developing, deploying and evaluating these systems. One of the prominent examples is the 2017 Human Rights Council resolution[163], which explicitly recognises the impact of profiling (which may involve the use of AI methods) to derive, infer or predict information about individuals for the purpose of evaluating some aspects about them. The Council also noted that 'individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights'. Another very recent example is the 2020 General Assembly Resolution on 'the right to privacy in a digital age'[164]. Among its key aspects, it expresses concern with respect to the increase in the development of biometric data-driven AI systems, including the rise of biometric identity programmes and scoring systems across the world. Furthermore, in July 2019, pursuant to the adoption of the Human Rights Council's resolution 'New and emerging digital technologies and human rights'[165], the Council's Advisory Committee was tasked with preparing a report to address the impact, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights, to be presented at the Council's 47th session in June 2021[166]. The aim of the study is also to map the progress made by the UN community in this area, as well the gaps in the current framework, with the prospect of further shaping the Council's digital agenda with respect to current (and future) AI-powered and data-driven technologies.

More specific issues pertaining to the use of AI and algorithmic systems have been addressed by several UN Special Rapporteurs. These reports often contain in-depth analysis of the most current challenges in this area, as well as suggestions for new lines of interpretation and possible amendments to the human rights regime. They also explain how AI technology may affect a broad spectrum of human rights. The most comprehensive example is a report[167] by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, examining the impact of AI on freedom of expression, privacy,

[159] UN Secretary General, 'Strategy on new technologies', 2018.
[160] UN, 'Secretary-General's High-level Panel on Digital Cooperation', 2020.
[161] UN HLPDC, 'The Age of Digital Independence', 2019.
[162] UN Secretary General, 'Roadmap for Digital Cooperation', 2020.
[163] UN Human Rights Council, 'The Right to Privacy in the Digital Age', Resolution A/HRC/34/L,7, 2017.
[164] UN General Assembly, 'Resolution A/RES/75/176', 2020.
[165] UN Human Rights Council, 'New and emerging digital technologies and human rights' , Resolution no. A/HRC/RES/41/11, 2019.
[166] UN Human Rights Council, 'New and emerging digital technologies and human rights'.
[167] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/73/348', 2018.

and non-discrimination. The report also proposes a human rights framework for the design and use of AI technologies by states and private actors. In particular, it urges for more transparency in the decision-making processes using algorithms and ensuring accountability mechanisms that would allow the challenge of such decisions in effective ways. Another example is a report[168] published by the Special Rapporteur on contemporary forms of racism, racial discrimination, and xenophobia. The report stresses that emerging digital technologies, driven by big data and AI, can reinforce and exacerbate existing inequalities, including those rooted in race, ethnicity, and national origin, in all areas of life, from education and employment, to healthcare and criminal justice. The report also corrects the misconception that these technologies are neutral and objective, by underlining that they are vulnerable for reproducing, whether intentionally or inadvertently, the discriminatory patterns of those developing, implementing, or using them. Last but not least, an important development responding to one of the most current challenges in the area of AI-powered biometric data collection systems is the report[169] by the Special Rapporteur on human rights and extreme poverty. The Rapporteur addresses the emergence of digital identification systems – a problem that, so far, has been only briefly tackled in the human rights legal framework. It describes the negative impact of those systems on privacy, non-discrimination, as well as several social and economic rights, warning against a grave risk of 'stumbling zombie-like into a digital welfare dystopia'[170]. A noteworthy conclusion drawn from all the three reports is that 'ethical approaches', which often govern the development and application of emerging digital technologies, 'must be pursued in line with international human rights law, and States must ensure that [they] do not function as a substitute for the development and enforcement of existing legally binding [human rights] obligations'[171].

In order to facilitate navigation though the key UN texts responding to challenges posed by new technologies, the UN has recently launched an online repository, the 'United Nations Hub for Human Rights and Digital Technology'[172], gathering relevant standards, analysis, and recommendations emerging from its human rights mechanisms.

Among regional human rights organisations, as already flagged, CoE has taken the most advanced approach in the field of AI and algorithmic systems. In addition to its main human rights instruments, such as the ECtHR and ESC, the organisation has developed two other binding conventions, which are particularly important in the context of the use of AI. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[173] ('Convention 108') was recently modernised by an amending protocol in 2018 ('Convention 108+')[174]. The Convention 'sets standards on the rights to privacy and data protection of individuals, regardless of technological evolutions'[175]. It is also the first and, to date, the only international legally binding instrument dealing with data protection. The amending protocol added a number of new principles to address challenges posed by the processing of personal data through technological development, the increasing flow of personal data, and the globalisation of processing operations. They include principles of transparency, proportionality, accountability, impact assessment, and respect for privacy by design. It also added new data subjects' rights, such as the right not to be subject to a decision significantly affecting a person based solely on an automated processing of their data, and

[168] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, op. cit.
[169] UN Special Rapporteur on extreme poverty and human rights, op. cit.
[170] UN Special Rapporteur on extreme poverty and human rights, op. cit., par. 72.
[171] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, op. cit.
[172] United Nations Hub for Human Rights and Digital Technology.
[173] Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', ETS No. 108, 1981.
[174] Council of Europe, Chart of signatures and ratifications of the Convention 108+.
[175] Council of Europe European Committee on Crime Problems (CPDC), 'Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law', 2020.

the right to obtain knowledge of the reasoning underlying such data processing where the results of this processing are applied. These new rights and principles are of particular importance in relation to the profiling of individuals and automated decision-making.

The process of modernisation for 'Convention 108' was carried out in parallel with other reforms to international data protection instruments, and alongside the reform of EU data protection rules, with the aim of ensuring consistency between both legal frameworks. As a result, Convention 108+ is mostly aligned with the EU General Data Protection Regulation provisions. Given that the Convention has been ratified by all CoE members and that is open for accession by states that are non-Contracting Parties of the CoE[176], as well as by international organisations, it has the potential to set global standards and serve as a vehicle for promoting a data protection approach consistent with the EU legal framework at global level[177]. The text of the Convention has been complemented by several guidelines developed by the Consultative Committee ('T-PD') established by the same treaty, which specify the application of its provisions to concrete situations, including in the context of AI and data protection[178], and big data[179].

The CoE's second binding international instrument particularly relevant for this study is the Convention on Cybercrime[180] ('Budapest Convention'). The Convention is important for criminalising offences against and by means of computers, for procedural powers to investigate cybercrime and secure electronic evidence, as well as for effective international co-operation in this area. It serves as a guideline for any country developing comprehensive national legislation against cybercrime. At the same time, the Convention is fully applicable to acts carried out or facilitated by AI systems, such as DDoS attacks or identity theft. The Budapest Convention is supplemented by a Protocol on xenophobia and racism committed through computer systems, while a new Protocol to the Budapest Convention on enhanced co-operation on cybercrime and electronic evidence is being prepared and may become available in 2021.

Furthermore, there has been a growing body of non-binding instruments developed by CoE institutions, which specifically tackle different applications of AI and their human rights impact. The most prominent examples are two recent documents adopted by the Committee of Ministers: the Recommendation on the human rights impacts of algorithmic systems[181] and the Declaration on the manipulative capabilities of algorithmic processes[182]. Moreover, a set of recommendations for national authorities concerning the use of AI in 10 main areas of action was adopted by the CoE's Commissioner for Human Rights[183]. Lastly, in 2017, the Parliamentary Assembly (PACE) adopted a recommendation on 'Technological convergence,

[176] To date, eight non-CoE countries are parties to the Convention: Argentina, Cape Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay. To date the 2018 amending protocol modernising the Convention has been ratified by Mauritius.
[177] Interview with Patrick Penninckx, Head of the Information Society Department of the Council of Europe, 08 January 2021.
[178] Council of Europe Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing (CoE T-PD), 'Guidelines on Artificial Intelligence and Data Protection', T-PD(2019)01, 25 January 2019.
[179] Council of Europe Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing (CoE T-PD), 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data', 2017.
[180] Council of Europe, 'Convention on Cybercrime', ETS No.185, 2001.; Council of Europe, 'Chart of signatures and ratifications of the Convention on Cybercrime'.
[181] Council of Europe Committee of Ministers, 'Recommendation on the human rights impacts of algorithmic systems', CM/Rec(2020)1, 2020.
[182] Council of Europe Committee of Ministers, Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes, 2019.
[183] Council of Europe Commissioner for Human Rights, 'Unboxing artificial intelligence: 10 steps to protect human rights', 2019. The areas of action include: human rights impact assessment; public consultations; human rights standards in the private sector; information and transparency; independent monitoring; non-discrimination and equality; data protection and privacy; freedom of expression, freedom of assembly and association, and the right to work; avenues for redress; and promoting knowledge and understanding of AI.

artificial intelligence and human rights'[184], followed by 7 reports in 2020 focusing on different AI-related thematic areas. They include the need for democratic governance of AI; the role of AI in policing and criminal justice systems; discrimination caused by AI; threats to fundamental freedoms; medical, legal and ethical challenges in the field of health care; consequences on labour markets; and legal aspects of 'autonomous vehicles'.

Besides that, the work of the CoE in the area of AI includes a number of research studies and reports developed by different CoE's specialised committees and expert bodies. One such example is the European Ethical Charter for the use of artificial intelligence in judicial systems[185], adopted by the European Commission for the Efficiency of Justice (CEPEJ). The Charter refers specifically to risks arising from AI-driven systems of anticipation of decisions, or risk-assessment systems in the judiciary, setting key principles for their use in this field. Other examples are the study on 'discrimination, artificial intelligence and algorithmic decision making'[186] commissioned by the European Commission on Racism and Intolerance (ECRI) or the Background Paper on 'AI and the media'[187].

It should be also emphasised that CoE's existing AI-related legal framework is likely to expand in the foreseeable future. Apart from several regulatory measures that are currently being considered in areas such as AI and criminal law[188] and AI-driven discrimination[189], there are also ongoing efforts to develop a (potentially binding[190]) legal instrument tailored to the specific challenges raised by AI systems and aimed at providing a comprehensive legal framework in this respect. This would challenge the current picture of a mostly fragmented existing legal framework composed of instruments focusing on particular aspects of different AI systems, and provide a more 'holistic' approach.

At the European level, the CoE's developments in AI are complemented by the recent work of the OSCE Representative on Freedom of the Media. This work focuses on the challenges posed by advanced automated tools and machine-learning systems in content moderation and distribution online[191]. The goal of the Representative's efforts is to ultimately develop policy recommendations on the most effective ways to safeguard freedom of expression and media freedom when using AI technologies within four main thematic areas of concern; security, hate speech, media pluralism, and surveillance.

**Box 7 : International human rights mechanisms undermined**

It should be flagged that the role of certain international human rights mechanisms in confronting repressive regimes has been undermined, as some authoritarian states have been gaining more influence on their agendas. Russia and China, the world's leaders in harnessing digital technologies for repression and social control, are currently both members of the UN Human Rights Council, but are believed to have used this and other UN forums as a 'means of shielding themselves from criticism, promoting their own illiberal projects', and 'reshaping international legal standards in ways that advance their interests'[192]. Both states have pushed for the adoption of a new global binding treaty on cybercrime, for example. This eventually resulted in a Russian-led

[184] Parliamentary Assembly of the Council of Europe (PACE), 'Technological convergence, artificial intelligence and human rights', Recommendation 2102 (2017), 2017.
[185] European Commission for the Efficiency of Justice of the Council of Europe (CoE CEPEJ), 'European Ethical Charter for the use of artificial intelligence in judicial systems and their environment', 2018.
[186] Zuiderveen Borgesius, F., op. cit.
[187] Council of Europe, 'Artificial Intelligence – Intelligent Politics Challenges and opportunities for media and democracy', Background Paper, 2020.
[188] Council of Europe European Committee on Crime Problems (CPDC), 'Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law', 2020.
[189] F. Zuiderveen Borgesius, p. 26., op. cit.
[190] CoE established the Ad-hoc Committee on Artificial Intelligence (CAHAI), which was tasked to examine the feasibility of a legal framework for the development, design and application of AI. See, CoE CAHAI, op. cit. p. 85.
[191] OSCE Representative on Freedom of the media, Impact of Artificial Intelligence.
[192] T. Ginsburg (2020), 'How Authoritarians Use International Law', Journal of Democracy, Vol. 31 Issue 4.

resolution[193] passed by the UN General Assembly in late 2019 which is an initiative that raises serious human rights concerns and 'advances Russia's long-standing goal to replace the Council of Europe's Budapest Convention'[194]. The new treaty would likely lack the standards balancing the interests of law enforcement and respect for fundamental rights provided by the Budapest Convention, instead facilitating the repression and censoring of political dissent online[195].

Other human rights organisations, such as the CoE, also face challenges in some of their member states that weaken the efficacy of their response to the trend of backsliding in human rights and democracy. The most prominent examples can be observed in Russia and Turkey; countries which refuse to uphold many of the organisations' legal standards and are among the leaders in failing to effectively implement the ECtHR's judgments, instead taking measures to undermine the Court's supremacy[196].

## 3.3 Surveillance in a digital age

The 'Snowden revelations' in 2013 have increased concerns about the negative impact of the interception of digital communications on human rights, and triggered numerous responses from different human rights institutions. In particular, surveillance has been a focus of several UN initiatives. A significant part of those responses has been built around the question of adapting the right to privacy to the challenges posed by new technologies. However, threats to freedom of expression, freedom of peaceful assembly, the right to non-discrimination and the right to effective remedy have been also addressed in this context.

At the UN level, the 'Snowden revelations' have triggered the emergence of 'the right to privacy in the digital age' discourse, which has led to numerous resolutions from the General Assembly[197] and Human Rights Council[198]. These documents reaffirm that human rights standards should apply to the interception of communications and collection of personal data, including certain types of metadata. It was concluded that aggregated metadata 'can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity'[199]. This discourse also resulted in the establishment of a dedicated UN special procedures mandate on the right to privacy[200], which closed a significant gap in the institutional

[193] UN General Assembly (2019), 'Countering the use of information and communications technologies for criminal purposes', Resolution A/RES/74/247

[194] J. Hakmeh, A. Peters (2020), 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet', Council on Foreign Relations, 13 January.

[195] T. Association for Progressive Communications (2020), Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online; Human Rights Watch (2021), 'Proposed UN Cybercrime Treaty Could Undermine Human Rights', 18 January.

[196] W. Bendek (2020), 'Are the Tools of the Council of Europe Sufficient to Protect Human Rights, Democracy and the Rule of Law from Backsliding?' European Convention on Human Rights Law Review, Volume 1: Issue 2; M. Yildirim (2020), 'Are Turkey's Restrictions on Freedom of Religion or Belief Permissible?', Volume 15: Issue 1-2; European Commission (2020), 'Key findings of the 2020 Report on Turkey'; T. Casier(2018), 'A Classic Dilemma: Russia's Threat to Withdraw from the Council of Europe', Heinrich Boell Stiftung, CoE Committee of Ministers (2020), 'Supervision of the execution of judgments and decisions of the European Court of Human Rights 2019', Expression Interrupted (2020) 'Freedom of Expression and Turkey: Implementation of ECtHR Judgments'.

[197] UN General Assembly, 'Resolution on the right to privacy in the digital age', A/RES/71/199, 2017.

[198] See e.g., UN General Assembly, 'The Right to Privacy in the Digital Age', Resolution 68/167, A/RES/68/167, 2013 or Resolution 28/16, A/HRC/RES/28/16, 2015. The list of all resolutions on the right to privacy in a digital age is available here: www.ohchr.org/EN/Issues/DigitalAge/Pages/InternationalStandardsDigitalPrivacy.aspx.

[199] U.N. General Assembly, 'Right to Privacy in the Digital Age', Resolution A/RES/73/179, 2018.

[200] UN General Assembly, 'The Right to Privacy in the Digital Age', Resolution 28/16, A/HRC/RES/28/16, 2015. The Special Rapporteur is an independent expert appointed by the Council to examine and report back on a country situation or a specific human rights theme. The Special Rapporteur is mandated to report on alleged violations of the right to privacy, including in connection with the challenges arising from new technologies.

human rights protection framework[201]. In their first report, the Special Rapporteur on the right to privacy outlined the main priorities issues pertaining to digital surveillance, as well as the role and responsibilities of companies to protect personal data[202]. Governmental surveillance, and in particular developing oversight mechanism of these activities, has remained an important focus of his subsequent reports[203]. The resolutions 'on the right to privacy in a digital age' and the work of the Special Rapporteur have since been complemented by a number of thematic reports from the other UN Rapporteurs[204] and the High Commissioner for Human Rights[205]. In all those documents, UN institutions elaborated principles to ensure that mass surveillance is conducted consistently with international standards, including standards of legality, necessity and proportionality, as well as robust procedural safeguards, such as independent oversight and the right to an effective remedy. These developments have been complemented by similar standards established at the regional level, in particular within CoE institutions[206] (with a particularly significant role of the European Court of Human Rights – ECHR[207]), the Inter-American Commission on Human Rights, and the African Commission on Human and Peoples' Rights[208].

More recently, the international human rights legal framework has responded to more targeted and offensive forms of surveillance, such as government hacking, both in national and exterritorial contexts[209]. At the same time, different institutions have promoted confidentiality, encryption, and anonymity as fundamental mechanisms to ensure human rights in the digital era[210]. This approach was confirmed by the ECtHR in one of its recent judgements[211]. Access to encryption and anonymity tools has been

[201] C. Nyst, T. Falchetta, 'The Right to Privacy in the Digital Age', *Journal of Human Rights Practice*, Vol. 9 (1), 2017 p. 109. African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (revised), 2019, Principle 40-41; the Declaration is a soft law document that interprets Article 9 (right to receive information and free expression) of the ACHPR and consolidates recent, digital age -related developments in this respect (including standards on privacy and protection of personal data in the context of communication) guided by hard-law and soft-law standards drawn from African and international human rights instruments and standards, as well as the jurisprudence of African judicial bodies.

[202] UN Special Rapporteur on the Right to Privacy, 'Report no. A/HRC/31/64', 2016.

[203] UN Special Rapporteur on the right to privacy, 'Report no. A/HRC/34/60', 2017; 'Report no. A/HRC/37/62', 2018.

[204] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 'Surveillance and human rights', Report no. A/HRC/41/35, 2019; 'Report no. A/70/361', 2015, 'Report no. A/HRC/23/40', 2013; UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism 'Report No. A/HRC/34/61', 2017.

[205] UN High Commissioner for Human Rights, 'Report on the right to privacy in the digital age', A/HRC/39/29, 2018; A/HRC/27/37, 2014. Both available at: www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalReports.aspx.

[206] Parliamentary Assembly of the Council of Europe, 'Resolution on Mass Surveillance 2045', 2015; Commissioner for Human Rights, Issue Paper on Democratic and Effective Oversight of National and Security Services (2015) and 'Positions on Counter-Terrorism and Human Rights Protection' (2015).

[207] ECtHR, 'Fact sheet on mass surveillance case law', 2020.

[208] OAS, Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15, 2015; 'Freedom of Expression and the Internet', 2013.

[209] UN High Commissioner for Human Rights, op. cit. 1028; UN General Assembly Resolution, A/RES/73/179, op. cit., 2018.

[210] Most recently in Human Rights Council, Resolution A/HRC/44/12, op. cit. Also in: UN General Assembly, A/RES/73/179, op. cit., 2018; UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Encryption and anonymity follow-up report', 2018; 'Report no. A/HRC/29/32', 2015.

[211] ECHR, *Engels v. Russia*, 61919/1623 June 2020. The case concerned the blocking of access to the applicant's website hosting information about filter-bypassing and anonymity-enhancing tools on the internet, such as VPN or the Tor browser, deemed dangerous by Russian authorities. In its judgements the ECtHR recognized the content-neutral nature of those technologies and rejected the argument that such technologies are solely used for extremist purposes, highlighting they may also serve legitimate purposes. It found therefore violation of, inter alia, Applicant's freedom of expression.

considered particularly vital for the work of journalists, human right defenders, civil society, journalists, whistle-blowers, and political dissidents facing persecution and harassment[212].

Furthermore, the role of the private sector in the context of state surveillance has been increasingly addressed. Initially, the human rights standards in this respect focused on situations in which private companies faced pressure from public actors. These included instances of States demanding excessive access to the massive amounts of information collected and stored by telecommunications and internet service providers, compelling private entities to assist in hacking operations, or calling for mandated back doors in encrypted communications[213]. More recent work addresses a growing industry of private surveillance tools (in particular, hacking tools and facial recognition technology). Many institutions have called on both state and non-state actors to refrain from providing surveillance equipment to foreign governments with a record of serious human rights violations, in the absence of legal safeguards or oversight mechanisms put in place[214]. The most comprehensive proposal for a legal and policy framework was provided by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, who called for an immediate moratorium on the global sale and transfer of such tools until rigorous human rights safeguards are implemented[215].

While excessive surveillance of digital communications remains a valid challenge, the most recent trends in developing a legal framework respond to the use of emerging surveillance technologies that involve processing of biometric data. This phenomenon has already been noted by several human rights institutions[216] and is likely to receive more attention in the future. A signpost for further developments in this area may be the recent standards regarding the use of facial recognition. In 2020, the UN Human Rights Council adopted a resolution specifically condemning the use facial recognition technology, alongside other digital tracking tools, in the context of the right to peaceful protests[217]. The Council noted that these technologies create a chilling effect on the exercise of the right to protest by enhancing governments' abilities to identify, monitor, harass, intimidate, and prosecute protesters. The Council, therefore, explicitly called on states to refrain from using facial recognition technology to arbitrarily observe individuals involved in peaceful protests. At the same time, unfortunately, it has not addressed the role of private sector actors, such as social media companies, in advancing respect for the right to peaceful assembly, even though they currently provide key tools for organising and covering demonstrations. Similar concerns regarding the use of facial recognition were expressed by the UN High Commissioner for Human Rights[218] and the U.N. Human Rights Committee in the newly-adopted General Comment No. 37 on the right to peaceful assembly[219]. At the same time, facial recognition has been addressed in other law

[212] UN General Assembly, 'Resolution on the safety of journalists and the issue of impunity', A/RES/72/175, 2017; UN Human Rights Council, 'Resolution on the safety of journalists', A/HRC/RES/39/6, 2018; UN High Commissioner for Human Rights, op. cit., 2018.
[213] UN General Assembly, A/RES/71/199, op. cit.; UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, op. cit., 2015; 'Report no. A/HRC/32/38', 2016; OAS, Special Rapporteur for Freedom of Expression of the Inter-American; Parliamentary Assembly of the Council of Europe (PACE), op. cit.
[214] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/HRC/41/35', 2019; UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Italy, Doc. CCPR/C/ITA/CO/6, 2017; Parliamentary Assembly of the Council of Europe, op. cit., 2015.
[215] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, op. cit., 2019.
[216] Such as UN General Assembly, A/RES/73/179, op. cit., 2018; UN High Commissioner for Human Rights, op. cit., 2018.
[217] UN Human Rights Council, 'Resolution on the promotion and protection of human rights in the context of peaceful protests', A/HRC/44/L.11, 2020.
[218] These conditions include effective, independent oversight of its use; strict privacy and data protection laws; and full transparency about the use of image recordings and facial recognition technology in the context of assemblies.
[219] UN Human Rights Committee, 'General comment no. 37 on the right of peaceful assembly (article 21)', 2020.Given that General Comments are important interpretive documents related to the human rights covered by the ICCPR, the new document has a significant potential to influence practical application of Article 21 by UN bodies. In particular, the Human

enforcement contexts. It is significantly covered in a report published in November 2020 by the Committee on the Elimination of Racial Discrimination recommending steps to prevent and combat racial profiling by law enforcement officials, for example[220].

Furthermore, as already flagged in the previous chapter, several human rights institutions acknowledged the negative impact of the COVID-19 pandemic on the right to privacy and data protection. Some of the UN Special Rapporteurs explicitly noted in this context that 'the virus is not just the cause of illness and death, it is also a pathogen of repression'[221], and that 'we could have a parallel epidemic of authoritarian and repressive measures'[222]. The current crisis has triggered unprecedented proliferation of human rights standards in the area of health-related surveillance systems. Several human rights institutions, both at the universal[223] and European[224] levels, adopted documents concerning the processing of health-related data for the purposes of combating the pandemic, addressing, among other things, the emergence of contact tracing apps. These documents point out the sensitive character of the processed data, and set minimal guarantees safeguarding rights to privacy and to protection of personal data that states should meet when deploying health surveillance mechanisms. They also emphasise that the emergency measures adopted in response the pandemic should not turn into standard practice. At the same time, the pandemic has increased the relevancy of pre-existing (but fairly recent) international standards and recommendations concerning the processing of health-related data. These include, for example, the CoE's Committee of Ministers Recommendation[225], or a report from the UN Special Rapporteur on the right to privacy[226], as well as general principles that should govern surveillance and are applicable in the pandemic[227].

## 3.4 Disruptions to free flow of information online

A growing body of findings and resolutions, both at the universal and regional levels, suggest that intentional disruptions to the internet violate international law. In 2015, in a joint declaration on freedom of expression and conflict situations, and UN and regional monitors of freedom of expression, declared that the 'filtering of content on the Internet, using communications "kill switches" (shutting down entire parts of communications systems) are measures which can never be justified under human rights law'[228]. At the

Rights Committee often relies on General Comments in the course of monitoring implementation of the ICCPR by its State Parties, including examination of periodic reports by governments.

[220] UN Committee on the Elimination of Racial Discrimination, 'Preventing and Combating Racial Profiling by Law Enforcement Officials', General recommendation No. 36, 2020.

[221] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Disease pandemics and the freedom of opinion and expression', Report no. A/HRC/44/49, 2020.

[222] S. Gebrekidan, 'For autocrats and others, coronavirus is a chance to grab even more power', New York Times, 30 March 2020.

[223] UN, 'Joint statement on data protection and privacy in the COVID-19 response', published by UN agencies: IOM, ITU, OCHA, OHCHR, UNDP, UNEP, UNESCO, UNFPA, UNHCR, UNICEF, UNOPS, UPU, UN Volunteers, UN Women, WFP and WHO, 2020; UN WHO, 'Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing', 2020; UN Special Rapporteur on the right to privacy, 'Report no. A/75/147', 2020.

[224] While responding to other pandemic-related threats, the other regional human rights legal framework have not addressed this particular issue. At the European level, the relevant standards have been developer mainly by the Council of Europe, including: (1) two Joint Statements 'on the right to data protection in the context of the COVID-19 pandemic' and on 'digital contact tracing' by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe; (2) CoE Secretary General, 'Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis: A toolkit for member states available in different languages', 2020; (3) CoE, 'Digital solutions to fight COVID-19', 2020, report analysing the impact on the rights to privacy and data protection of the measures taken to prevent the spread of the COVID-19 pandemic in the 55 African, Latin-American and European countries Parties to Convention 108.

[225] CoE Committee of Ministers, 'Recommendation CM/Rec (2019)2 on the protection of health-related data', 2019.

[226] UN Special Rapporteur on the right to privacy, 'Report no. A/74/277', 2019.

[227] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/44/49, op. cit., 2020.

[228] Available at: www.osce.org/fom/66176.

UN level, the importance of access to online information has been confirmed in numerous documents. The landmark instrument specifically condemning internet shutdowns is the Human Rights Council Resolution from 2016[229]. Since then, calls on states to refrain from imposing internet or telecommunications network disruptions have been repeated on several occasions[230]. One of the most recent examples is the resolution of the Human Right Council, which expressed deep concern about the imposition of this measure as a means to undermine peaceful protests[231]. The importance of the free flow of online information in the context of the right to peaceful assembly was also recently stressed by the ECHR[232]. Among other regional responses to internet shutdowns, given network disruptions have lately become more prevalent in Africa, it is particularly noteworthy to mention steps taken in this respect by the African Commission on Human and Peoples' Rights[233]. It specifically recognised that 'universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression [and] access to information' in a revised version of the Declaration of Principles of Freedom of Expression and Access to Information in Africa, which was adopted in 2019. Moreover, the African Special Rapporteur on Freedom of Expression and Access to Information[234] expressed concern about the continuing trend of internet shutdowns in Africa, in particular in Chad, Sudan, the Democratic Republic of Congo, Gabon, and Zimbabwe. Furthermore, a landmark judgment was delivered by the Community Court of Justice of the Economic Community of West African States (ECOWAS), which held that the Togolese government violated the applicants' right to freedom of expression by shutting down the internet during protests in September 2017[235]. Still, despite all these efforts, internet shutdowns remain on the agenda of human rights institutions as one of the key challenges for freedom of expression for the next decade[236].

Apart from internet shutdowns, other forms of disruption to the dissemination of online information have been condemned in international law, including imposing measures to unlawfully or arbitrarily block content or take down media websites (including via DDoS attacks)[237]. A comprehensive set of standards concerning blocking access to websites was recently provided by the ECtHR in four cases against Russia[238]. Moreover, human rights institutions developed recommendations preventing governments from putting undue pressure on internet intermediaries (including large online platforms) to remove content or enable excessive access of the authorities to user data. These recommendations include certain procedural guarantees safeguarding transparency, legality, necessity and proportionality of the governments'

[229] UN Human Rights Council, 'Resolution A/HRC/32/L.20', 2016.
[230] For example: UN HRC, 'Resolution on Freedom of Opinion and Expression', A/HRC/44/12, 2020; Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/HRC/35/22', 2017.
[231] UN Human Rights Council, 'Resolution A/HRC/44/L.11', 2020.
[232] ECtHR, *Kablis v. Russia*, 59663/17, 30 April 2019. The ECtHR held the prohibiting the Applicant from holding a demonstration, and ordering the removal of his online posts about it, as well as entire social media account, violated his rights to freedom of expression and public assembly.
[233] African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (revised), op. cit., 2019.; see also: '362 Resolution on the Right to Freedom of Information and Expression on the Internet in Africa' - ACHPR/Res.362(LIX)2016, 2016.
[234] African Special Rapporteur on Freedom of Expression and Access to Information, 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the situation of freedom of expression and access to information in the Republic of Zimbabwe', 2019; 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa', 2019.
[235] ECOWAS, Amnesty International & Others v. The Togolese Republic, ECW/CCJ/JUD/09/20, 25 June 2020.
[236] UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Challenges to Freedom of Expression in the Next Decade', 2019.
[237] For example, in its resolution 39/6, the UN Human Rights Council condemned these activities in the context of journalistic work.
[238] ECtHR, *OOO Flavus and Others v. Russia*, 12468/15 and 2 others; *Bulgakov v. Russia*, 20159/15; *Engels v. Russia*, op. cit.; *Vladimir Kharitonov v. Russia*, 10795/14 (all judgments delivered on 23 June 2020).

demands, including (in principle) an obligation to obtain an order from a judicial authority (or other independent authority whose decisions are subject to judicial review), as well as establishing a mechanism for an effective remedy[239]. Both with respect to content restriction and disclosures of personal data, there should be a reporting obligation for states to publish comprehensive information on the number, nature, and legal basis of such orders. International standards also explicitly prohibit States to exert pressure on internet intermediaries through non-legal means. In addition, demands to access personal data stored by internet intermediaries should meet international data protection principles prescribed, for example, in Convention 108+, such as purpose limitation, data minimisation, storage time limitations, data security, and data subjects' right. States should ensure that the right to confidentiality of all private communications extends not only to the content of the communication, but also to metadata.

In 2020, several human rights institutions developed guidelines addressing specific threats to freedom of expression online posed by the COVID-19 pandemic, emphasising the need to protect access to accurate and reliable information in times of crisis. The most elaborate document is the report of the UN Special Rapporteur on freedom of expression, which focuses on 5 challenges during the pandemic:

1) access to information held by public authorities;
2) undisrupted access to the Internet;
3) protection and promotion of independent media;
4) the need to counteract public health disinformation;
5) the rise of public health surveillance[240].

In addition to freedom of expression risks, the Rapporteur also highlighted the negative impact of network disruptions imposed in the course of the pandemic on the right of everyone to enjoy the benefits of scientific progress, protected under article 15 (1) (b) of the CESCR. The importance of access to the Internet during the crisis in the context of economic, social and cultural rights has also been emphasised in the resolution of the Inter-American Commission on Human Rights[241] and in the joint statement with IACHR Special Rapporteur for Freedom of Expression[242]. At the same time, freedom of expression monitors from the UN, OSCE and OAS addressed the problem of punitive actions against journalists for pandemic-related speech, and stressed that press freedom must not be undermined by measures to counter disinformation about COVID-19[243]. In particular, penalisation of disinformation should not be accepted as a proportionate measure, 'failing to achieve its goal of tamping down information while instead deterring individuals from

[239] COE Committee of Ministers, 'Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries', 2018; African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (revised), op. cit., 2019; UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/HRC/38/35, 2018.
[240] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2020), 'Report: Disease pandemics and the freedom of opinion and expression', A/HRC/44/49.
[241] Inter-American Commission on Human Right, 'Pandemic and human rights in the Americas', Resolution no. 1/2020, 2020.
[242] Inter-American Commission on Human Rights and IACHR Special Rapporteur for Freedom of Expression, 'States of the Region must Accelerate Universal Internet Access Policies during the COVID-19 Pandemic and Adopt Differentiated Measures to Incorporate Groups in Vulnerable Situations', 2020.
[243] IACHR Special Rapporteur for Freedom of Expression, UN Special Rapporteur on freedom of expression, and OSCE Representative on Freedom of the Media, 'COVID-19: Governments must promote and protect access to and free flow of information during pandemic – International experts', Press release 58/20, 2020.

sharing what could be valuable information'[244]. Similar concerns have been expressed in this respect by the CoE's Commissioner for Human Rights[245].

Additionally, one of the main threats to online free expression recognised by human rights institutions is different forms of cyberviolence, in particular state-sponsored harassment campaigns. Until recently, the work of international organisations in this area had focused on developing general standards on combating hate speech[246] or increasing protection for the most vulnerable groups, such as journalists[247]. In recent years, however, there has been an increasing number of international initiatives addressing discrimination and violence against women in the digital context. In 2017, the UN General Assembly unequivocally condemned all 'specific attacks on women journalists in the exercise of their work, including sexual and gender-based discrimination and violence, intimidation and harassment, online and offline'[248]. The problem was tackled more extensively in the 2018 resolution of the Human Rights Council[249], and in the report of the Special Rapporteur on violence against women, its causes, and consequences[250]. Important work has been done in this area, not only in terms of setting policy guidelines, but also in advancing research about the problem by UNESCO[251] and the OSCE Representative on Freedom of the Media[252] (in particular, with respect to online violence against female journalists). In addition, two binding instruments developed within the Council of Europe, namely the Budapest Convention and the Istanbul Convention[253], should be flagged as important developments in the context of countering gender-based cyberviolence, even though it has been pointed out that these instruments may not address the specificities of violence in cyberspace in a satisfactory manner[254]. By the same token, the CoE's Committee of Ministers Recommendation on preventing and combating sexism can be also relevant[255].

Last but not least, while governments across the world still increasingly resort to shutting down the internet, other network disruptions, or online harassment campaigns, recently many human rights institutions have been turning their attention to threats to free speech related to the activity of non-state

[244] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/44/49, op. cit., 2020.
[245] CoE Commissioner for Human Rights, 'Press freedom must not be undermined by measures to counter disinformation about COVID-19', 2020.
[246] 'Hate crime is partly covered by the Additional Protocol to the Budapest Convention on Xenophobia and Racism, and thus addresses cyberviolence motivated by certain biases, but not if motivated by other perceived characteristics such as gender, sexual orientation or disability. The work of the Council of Europe and other organisations on discrimination and intolerance is also relevant. Key issues are the role of service providers and the question of hate speech versus free speech'. See CoE, Online hate speech
[247] An example may be CoE's recommendation on the protection of journalism and safety of journalists and other media (2016) which provides specific guidelines to member States on addressing this trend. Moreover, since 2012, the Human Rights Council has considered resolutions on the safety of journalists every two years, with each iteration of the text setting increasingly progressive standards, including in the context of online environment.
[248] UN General Assembly, 'Resolution on the safety of journalists and the issue of impunity', A/RES/72/175, 2017.
[249] UN Human Rights Council, 'Resolution on accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts', A/HRC/38/L.6, 2018.
[250]UN Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, 'Report no. A/HRC/38/47', 2018.
[251] ICFJ-UNESCO, 'Global Study: Online Violence Against Women Journalists. A Global Snapshot of Incidence and Impacts', 2020; ICFJ (2020), 'ICFJ-UNESCO Global Study: Online Violence Against Women Journalists': 'UNESCO and the International Centre for Journalists (ICFJ) have conducted a global survey to assess the scale and impacts of online violence targeting women journalists, and to help identify solutions to this pernicious problem. The survey in focus in this report is part of a broader UNESCO-commissioned collaborative study examining the incidence, impacts and responses to online violence against women journalists in 15 countries'.
[252] OSCE, 'Safety of Female Journalists, Resource guide', 2020; 'Recommendations on Countering Online Abuse of Female Journalists', 2015; 'Communiqué by the OSCE RFoM on Media Pluralism, Safety of Female Journalists and Safeguarding Marginalized Voices Online', 2019.
[253] CoE, 'Convention on preventing and combating violence against women and domestic violence', CETSNo.210, 2011.
[254] CoE Cybercrime Convention Committee (T-CY), 'Mapping study on cyberviolence', 2018.
[255] CoE Committee of Ministers, 'Recommendation on preventing and combating sexism', CM/Rec(2019)1, 2019.

actors, in particular large online platforms. In the joint declaration by freedom of expression monitors from the UN, OSCE, OAS and ACHPR, 'a private control over online information flow' is considered one of the main challenges to the freedom of expression for the upcoming decade[256]. At the same time, online platforms are in a 'unique position to prevent or mitigate risks that may be inflicted by users' illegal activity'[257]. At the moment, the vast majority of international standards which aim to address this problem focus on content moderation[258]. In particular, there are recommendations for States on how intermediaries' liability regimes should be shaped at the national level. According to those standards, while in principle intermediaries should cooperate with states to effectively secure the restriction of illegal content, they should also benefit from limited liability regimes. States should refrain from imposing obligations to use general content monitoring to pro-actively identify illegal user-generated content in national laws[259]. Moreover, there are recommendations regarding the need to adhere online platforms' internal policies to international freedom of expression standards, and provide 'due process' safeguards for users, as well as independent, external oversight of the take down decisions, including those made on the basis of the companies' own terms and conditions[260]. There is also a growing body of recommendations concerning the use of automation in content moderation. These refer, in particular, to the need for increasing transparency of algorithms used for this purpose, and to possible limitations for their application due to the 'deleterious impact', which a sole reliance on these tools may have on human rights[261]. Moreover, as already flagged in the section on AI, human rights institutions have been increasingly addressing the use of algorithms for broader content governance which enables companies to 'curate search results and newsfeeds as well as advertising placement, organising what users see and when they see it'[262].

## 3.5 Human rights and private actors

A transformative feature of the digital communications environment which transpires not only from the previous section, but the entire study, is the impact of private companies on human rights in digital space[263]. As already mentioned, this applies especially to internet intermediaries, including, in particular, large, dominant online platforms operating globally, such as social media or search platforms. Additionally, the international human rights legal framework puts a spotlight on the private surveillance tools industry. The role of both kinds of these non-state actors has been emphasised in most of the issue-specific instruments discussed earlier in this chapter (however, as highlighted above, some of these instruments still fail to appropriately address the significance of private sector[264]).

Much of the literature on human rights considers that the framework applies primarily to state actions. The states' duties extend beyond the obligation to respect, however, and also include 'positive' measures to

[256] UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Challenges to Freedom of Expression in the Next Decade', 2019.
[257] B. Bukovska, 'Spotlight on Artificial Intelligence and Freedom of Expression #SAIFE', OSCE, 2020.
[258] COE Committee of Ministers, op. cit., 2018; UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/HRC/38/35, op. cit., 2018.
[259] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, op. cit., 2018; COE Committee of Ministers (2018), op. cit., 2018.
[260] Ibidem.
[261] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Disease pandemics and the freedom of opinion and expression', Report no. A/HRC/44/49, 2020; Report no. A/73/348, op. cit. 2018; COE Committee of Ministers, op. cit., 2018.
[262] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/73/348, 2018, Ibidem; see also: COE Committee of Ministers, ibidem., 2018.
[263] UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Challenges to Freedom of Expression in the Next Decade', op. cit., 2019.
[264] See UN Human Rights Council, A/HRC/44/L.11, op. cit., 2020, discussed in the section 'Surveillance in a digital age'.

protect the enjoyment of rights against threats emanating from private actors[265]. In the context of AI, for example, this implies that 'states can meet this obligation through legal measures to restrict or influence the development and implementation of AI applications, policies regarding the procurement of AI applications from private companies by public sector actors, self-and co-regulatory schemes or building of capacity in private sector companies to recognise human rights in their corporate endeavours'[266]. Similarly, with respect to the export of surveillance technologies by private actors, states should have export control regimes in place, which 'assess the legal framework governing the use of this technology in the destination country, the human rights record of the proposed end user, and the safeguards and oversight procedures in place for the use of surveillance powers. Human rights guarantees need to be included in export licensing agreements'[267].

Even though international human rights law acknowledges that states are the prime duty bearers in the context of human rights obligations, many standards recognise that the private sector also bears a responsibility to respect human rights. The main global standard in this respect has been provided by the UN in the Guiding Principles on Business and Human Rights[268]. The Guiding Principles offer a universal, non-binding vehicle for applying human rights standards to corporations. They build upon and help to operationalise the 2008 'Protect, Respect and Remedy' Framework developed by the UN Special Representative on the issue of human rights and transnational corporations and other business enterprises, corresponding to three pillars for action (see Box 8).

**Box 8: Three pillars of the of the 'Protect, Respect and Remedy' Framework**

**I. Protect** - focusing on states' duty to protect against human rights abuses by third parties, including business, through appropriate policies and regulation.

**II. Respect** - focusing on corporate responsibility to respect human rights which means that companies must inter alia prevent and mitigate human rights harms, develop policies that promote human rights, carry out due diligence to assess human rights risks and address adverse impacts that occur.

**III. Remedy** - focusing on both State and business responsibility to provide victims with an access to effective remedy, both judicial and non-judicial.

The Guiding Principles apply to all kind of businesses, including online platforms and other tech companies. However, since they are not specific to the tech industry, companies may face practical problems with their effective application. In order to facilitate application of the principles to this particular sector, several human rights documents include guidelines on both substantive standards and processes for implementing them, for example in the algorithmic systems domain[269]. In addition, there are other ongoing efforts within the UN, such as the 'Business and Human Rights in Technology Project' ('B-Tech

[265] See e.g., article 2 (1) of the ICCPR and also 'The Guiding Principles on Business and Human Rights' ('State duty to protect human rights').
[266] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/73/348', op. cit., 2018.
[267] UN High Commissioner for Human Rights, Report no. A/HRC/39/29, 2018, op. cit.; see also UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/HRC/41/35, op. cit., 2019.
[268] The Guiding Principles on Business and Human Rights: Implementing the UN 'Protect, Respect and Remedy' Framework developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. See, Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, 'Report. No. A/HRC/8/5', 2008. The UN Human Rights Council endorsed the Guiding Principles in its resolution 17/4 (2011). The Principles are often invoked not only by UN bodies but also other human rights institutions operating on the regional level, for example: COE Committee of Ministers, op. cit., 2018.
[269] CoE Committee of Ministers, op. cit., 2020; UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/73/348, op. cit., 2018.

Project') which applies the Guiding Principles to digital technologies[270]. Another initiative is the 'Accountability and Remedy Project' launched in 2014 by the UN High Commissioner for Human Rights. It aims to deliver workable recommendations for more consistent implementation at the national level of the guiding principles in the area of access to remedy in relation to non-state actors, including, for example, with respect to abuses of the right to privacy in the digital space[271]. To date, three phases of the project have been completed in which recommendations concerning establishing or improving three categories of grievance mechanisms referred to in the UN Guiding Principles were developed:

- judicial mechanisms;
- state-based non-judicial mechanisms;
- non-state based grievance mechanisms.

Following up on that work, the UN High Commissioner for Human Rights began work on a fourth phase in 2020 focusing on enhancing the accessibility, dissemination and implementation of the findings and recommendations made in the previous phases.

At the same time, there are ongoing efforts at the UN to complement the Guiding Principles on Business on Human Rights with an international legally binding treaty[272] regulating corporate liability for human rights abuses. The currently negotiated 'Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises' addresses the need to increase the effectiveness of human rights protections in this area, which at the moment is undermined by its non-mandatory nature and lack of a central mechanism to ensure their implementation[273]. The limited effectiveness of this framework can indeed be observed specifically in the technological domain. On the one hand, a growing number of companies are making formal commitments to human rights, including explicitly to upholding the standards established in the UN Guiding Principles. According to the Ranking Digital Rights Corporate Accountability Index 2020[274] (see Box 7) all the U.S.-based large online platforms (see Box 4 in Chapter 3) performed relatively well in 2020 when it came to declaring respect for human rights principles (while their Chinese counterparts, even though ranked much lower, also made some progress in this respect[275]). On the other hand, however, most companies scored poorly on practical implementation of these commitments, including human rights due diligence, regular engagement with civil society, and offering effective remedy mechanisms for addressing human rights harms.

**Box 9: Civil society and multistakeholder initiatives on business & human rights in a digital space**

In addition to the above-mentioned standards, there are a range of civil society and multistakeholder initiatives that have developed recommendations that support operationalising the UN Guiding Principles for companies in the digital environment or monitoring their effective implementation. These include, for example:

- **Global Network Initiative**[276] – A multistakeholder initiative dedicated to advancing human rights in the information and communications technology sector. It has developed a set of

[270] Information on the B-Tech Project is available here.
[271] OHCHR Accountability and Remedy Project; the Project has received multiple mandates from the Human Rights Council (Resolutions 26/22, 32/10, 38/13 & 44/15).
[272] The elaboration of the Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises was mandated in 2014 by Resolution 26/9 of the UN Human Rights Council. The Second Revised Draft of the instrument was published in August 2020 and is undergoing negotiations. By the end of July 2021 third revised draft text shall be presented, which will form the basis of negotiations later that year.
[273] B. Faracik, 'Implementation of the UN Guiding Principles on Business and Human Rights', 2017, p. 13.
[274] Ranking Digital Rights, 'Ranking Digital Rights Corporate Accountability Index 2020', 2021.
[275] R. MacKinnon, 'Chinese tech giants can change: But the state is still their number one stakeholder', 2021.
[276] Global Network Initiative, available at https://globalnetworkinitiative.org/.

principles ('GNI Principles') and implementation guidelines to 'guide responsible company, government, and civil society action when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users[277].

- **Toronto Declaration**[278] – A set of standards protecting human rights in the age of artificial intelligence, focusing on protecting the rights to equality and non-discrimination in machine learning systems, developed by civil society organizations working on digital rights.
- **Santa Clara Principles**[279] – A set of standards 'outlining minimum levels of transparency and accountability that online platforms should provide around their moderation of user-generated content[280], drafted by a group of organizations, advocates, and academic experts who support the right to free expression online.
- **Ranking Digital Rights Corporate Accountability Index**[281] – An index evaluating 'the world's most powerful digital platforms and telecommunications companies on their disclosed policies and practices affecting users' rights to freedom of expression and information and privacy'.

## 3.6 Conclusions

The recent developments in the human rights framework described in this chapter are a sign of a growing awareness among the international community of how technologies affect societies and almost every part of our day-to-day lives. They also demonstrate an increasing caution and healthy scepticism towards application of new technologies, as it has been acknowledged that, alongside potential advantages, there may be unintended adverse consequences, or sometimes the potential to be used as deliberate tools of repression. The existing legal framework tackles many threats identified in Chapter 3, including practices described as part of a 'next generation repression toolkit'. In particular, it responds to problems such as internet shutdowns and other network disruptions, mass and biometric surveillance, government hacking, export of surveillance tools, or cyber harassment. At the same time, there are fields that can be improved or should be further addressed. The main conclusions, built on the analysis of existing norms and interviews with different stakeholders[282], have been listed below with the aim of informing discussions on future development of human rights protection in the digital era.

Among the new and emerging technologies, which may be used for repression and social control, AI and algorithmic decision-making systems have dominated the most current agendas of human rights organisations. Building upon general principles on personal data protection, the right to privacy, freedom of expression or non-discrimination, there have already been several soft law instruments and other initiatives that aim to respond to the certain threats posed by those technologies. The existing instruments focus mainly on particular technological applications of AI technologies or their impact on selected rights. Still, there are gaps in the current level of protection. Most importantly, a comprehensive, international legal instrument, specifically tailored to challenges posed by AI, is lacking[283]. At the same time, there are already advanced debates on how this gap could be filled. There seems to be a consensus that such an

[277] GNI, 'Global Network Initiative Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 2015
[278] Amnesty International and Access Now, 'The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems', 2018.
[279] Santa Clara Principles on Transparency and Accountability in Content Moderation (2018), currently under review process.
[280] York, J. C., 'The Santa Clara Principles During COVID-19: More important than ever', Electronic Frontier Foundation, 2020.
[281] Ranking Digital Rights, op. cit.
[282] See Section 2.2. 'Note on the methodology' and Annex 7.2.
[283] Council of Europe Ad Hoc Committee on Artificial Intelligence (CoE CAHAI), op. cit., 2020.

instrument should be technology neutral and reflect paradigm shifts in AI technologies. In particular, it should incorporate human rights safeguards into the entire life cycle of these technologies, including their design, deployment and implementation, as well as to the entire 'datafication cycle' (a process whereby data about individuals and things is collected, transmitted, and used to guide decision-making in the real world[284]). There is also an urgent need to further address the causes and impact of unintended bias and discrimination resulting from certain algorithmic and automated decision-making based on AI[285]. It is particularly important in contexts such as predictive policing in law enforcement, distribution of access to vital products and services or certain privileges, and content governance online[286].

It should also be noted that new technologies, in particular those driven by AI, challenge the traditional concept of groups particularly vulnerable to human rights violations, and (to some extent) the whole concept of a 'victim' and 'harm' under human rights framework. On the one hand, the analysis of trends in Chapter 2 has shown that 'traditional' groups such as racial, religious, or sexual minorities, political opposition, or civil society activists remain the primary targets. On the other hand, the rise of, for example, digital welfare systems, has exposed new, but also more 'blurred', groups that may be particularly affected, such as the poor and other disadvantaged categories. In addition, measures such as algorithmic surveillance affect large parts of populations, if not whole societies, and thus the targets can no longer be specifically identified. Moreover, the individual harm is more difficult to grasp and often practically impossible to be documented or proved. The traditional notions of 'victim' status or 'harm' may therefore be insufficient to meet the current challenges posed by new technologies, and may require revisiting in order to offer effective human rights protection to individuals in a digital age[287].

At the same time, there has been an increasing recognition among human rights institutions that new and emerging technologies may impact a broad range of human rights. Such a 'holistic' approach, rather than focusing on the impact on particular rights, which were more prevalent in the past, should be kept and further expanded. It is difficult, for example, to comprehensively address the threats related to cyberviolence without considering at the same the time human rights implications of automatisation of online content moderation. Similarly, one should not push for improving responses to cybercrime, including effective identification of perpetrators of online crimes, without due regard to the value of anonymity and encryption in certain contexts. All these issues, at least to some extent, have been addressed in the existing human rights framework, but often in a fragmented way, without taking into consideration interrelations between them[288]. Moreover, while to date civil and political rights were under the spotlight of the human rights community, it has become clear that a number of social, economic and cultural rights are also severely affected. Technology-related violations of these rights have become particularly apparent alongside proliferation of digital identity systems and in the context of the COVID-19 pandemic. In light of these developments and in line with the 'holistic' approach, social, economic, and cultural rights should be given more prominence in future human rights organisations' agendas on new technologies[289].

[284] Interview with representative of international institution, 14 January 2021, CoE CAHAI (2020), ibidem.
[285] UN Secretary General, 'Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights', A/HRC/43/29, 2020.
[286] CoE Commissioner for Human Rights, 'Speech at the conference Human Rights in the Era of AI Europe as international Standard Setter for Artificial Intelligence', 20 January 2021.
[287] E. Kosta, 'Algorithmic state surveillance: Challenging the notion of agency in human rights', *Regulation & Governance*, 7 July 2020.
[288] An example may be the recent UN Human Rights Council Resolution on Freedom of opinion and expression, which fails to address the impact of surveillance technologies, which cause significant chilling effect on freedom of expression (A/HRC/44/12).
[289] CoE Commissioner for Human Rights, 'Speech at the Human Rights talk: COVID-19 and Human Rights – Lessons learned from the pandemic', 10 December 2020.
UN Secretary General, A/HRC/43/29, 2020, op. cit.

In 2020, several human rights institutions developed guidelines addressing human rights threats posed by the COVID-19 pandemic, including those specifically related to the use of new technologies. In particular, they address the rise of health-related surveillance tools, such as mobile phone apps developed to tackle the pandemic, and a number of freedom of expression risks. A concerning trend of governments using the pandemic as a pretext to expand general surveillance in order to increase repression and social control was also noted. Looking to the future, the important role of the human rights community is to further monitor the situation and, as more evidence is available, continue assessment of COVID-19-related surveillance's impact on human rights. In particular, it is important to urge that any current measures justified by governments through the health emergency remain temporary, time-limited, and take the least intrusive approach. Based on lessons learned during the current crisis and keeping in mind that pandemics may become episodic features of contemporary life, human rights organisations should also work towards more sustainable and evidence-based guidelines on health-related emergency measures to prevent the future abuse of surveillance technologies. At the same time, it has to be acknowledged that COVID-19 pandemic is a point of no return. It has most likely already contributed to a wider normalisation of surveillance, and thus the human rights community will have to confront challenges arising from that fact.

It has been also widely recognised that an effective human rights response to the challenges posed by new technologies will not happen without the involvement of private companies. This applies, in particular, to large, dominant online platforms that, by exploiting huge volumes of user data for their business-driven purposes and exercising private control over the flow of online information, hold enormous power in the digital environment, posing systemic threats to a wide range of human rights. At the same time, the role of other corporations in facilitating human rights violations related to the use of new technologies, such as those producing and selling surveillance equipment, should not be overlooked. It is therefore urgently required of the private sector in the technological domain to act responsibly in mitigating the risks that their activities may have on human rights. Currently, the main global standard for applying human rights responsibilities to corporations has been provided by the UN Guiding Principles on Business and Human Rights. However, the Guiding Principles do not sufficiently address the specificities of new business models that have arisen in the new technologies sector, which may impede their effective application in this area[290]. It is therefore important to develop more practical guidance on the application of the Guiding Principles to digital technologies. Those developments should build on existing initiatives, such as the B-Tech Project or 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights'[291] published by the European Commission. Additionally, improving mechanisms of cooperation and information-sharing between human rights community and technological companies could also facilitate better adherence of those actors to their human rights responsibilities. The non-binding character of this framework remains an impediment to fully effective protection against human rights abuses related to the activities of the private sector, which is why ongoing efforts to develop a mandatory international legal instrument (such as the UN Legally Binding Instrument to regulate the activities of transnational corporations and other business enterprises) should be supported.

Apart from enhanced cooperation with the corporate sector, it is also essential to include other actors, particularly from civil society and academia. First of all, with their field experience and expertise, these actors may inform international responses to the actual negative impacts of new technologies at the national level. Second, given the already existing initiatives, such as the Toronto Declaration[292] or Santa Clara Principles[293], they may provide valuable input to the process of looking for solutions to the problems

[290] Interview with representative of international institution, 14 January 2021.
[291] Shift and the Institute for Human Rights and Business, 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', European Commission.
[292] Amnesty International and Access Now, The Toronto Declaration, op. cit.
[293] Santa Clara Principles on Transparency and Accountability in Content Moderation, op. cit., 2018.

diagnosed in this section. Thirdly, this community also has a significant role in promoting international human rights standards in domestic policymaking.

Moreover, human rights should not give way to ethical frameworks in the field of new technologies. While ethical frameworks have been increasingly prevalent, in particular in the AI domain, and may assist with working through particular challenges regarding concrete applications of this technology, they do not provide tangible protection for individuals. Therefore, they should not be considered a substitute for a binding, actionable, and well-established human rights legal framework[294]. Both public and private actors developing and implementing ethical codes on AI should ensure that they are grounded in human rights principles, in line with guidance that should be provided, in this respect, by the human rights community.

There are also other kinds of gaps that impede tackling the challenges posed by new technologies. Responding to complex human right issues created by these technologies requires adequate resources, including, in particular, human resources to close the 'knowledge gap' between legal/human rights and technology experts[295]. Human rights bodies should therefore encourage more participation from diverse actors, including technology experts and representatives of the private sector who design and produce technologies. It is necessary to build new principles that can accommodate more varied and comprehensive perspectives. Additionally, as new technologies continue to unfold; this goal will not be met without allocating appropriate funds to facilitate further research in this area[296]. Last but not least, some respondents in our study have emphasised that the key limitation of the human rights legal framework is not the question of its content, but of its often-ineffective application at the national level, with limited avenues for remedies for harm caused by human right violations[297]. More specifically, in the context of the dynamic expansion of technologies, it has been suggested to establish an emergency-response mechanism that would allow a more timely reaction of the international community to emerging digital threats[298]. Finally, the increasing influence of non-democratic regimes on the agenda of human rights institutions and on the shape of international legal standards further undermines the role of this framework.

# 4 The EU's democracy and human rights toolbox

This chapter lays out the policy instruments the EU has at its disposal to support democracy and human rights across the world, paying particular attention to those parts of its toolbox related specifically to the effects of digital repression. The chapter describes how the EU has deployed the different parts of its policy toolbox in recent years. It concludes with an assessment of these policy approaches and relates them to the multiple digital trends summarised in the foregoing chapters. The chapter finds that the EU has moved up a gear in its efforts to tackle digital challenges, but that the worrying trends described in Chapter 3 require it to work even harder to improve its toolbox. While previous chapters highlight the spread of a multi-faceted set of digital problems, the EU's external toolbox has improved mainly on select elements of this; in particular, it has focused on the use of digital technologies for repression against democracy and human rights actors within civil society, the export of security surveillance equipment, and the transnational use of digital tactics against the EU itself. The more subtle forms of social control, advanced

[294] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/73/348, op. cit., 2018.
[295] Interview with representative of international institution, 14 January 2021.
[296] Interview with representative of international institution, 14 January 2021.
[297] Interview with Juan Carlos Lara, Research and Policy Director, Derechos Digitales, 09 December 2020; Interview with Gaspar Pisanu, Latin America Policy Manager, Access Now, 6 January 2021; Diego Naranjo, Head of policy, European Digital Rights, 08 January 2021; Jonathan McCully, Legal Adviser, Digital Freedom Fund, 17 December 2020.
[298] Interview with Juan Carlos Lara, Research and Policy Director, Derechos Digitales, 09 December 2020.

AI techniques, or health-related controls described in Chapter 3 have so far proven less amenable to being incorporated fully into foreign policy instruments.

## 4.1 General evolution of the EU toolbox

### 4.1.1 Evolution of the core toolbox

The EU has been adding to and fine-tuning its array of human rights and democracy policy instruments for nearly three decades. The Union first began to develop funding instruments on these issues within its external aid in the early 1990s. From the mid-1990s, the EU insisted that all third-country partners sign a so-called 'essential elements' clause as part of formal contractual agreements with the Union, committing them to respect democratic norms and human rights standards. In the 1990s and early 2000s, the EU's commitments intensified as democracy spread globally, and the Union offered assistance to the many governments that committed themselves to political reform. As this stage, the enlargement process in Central and Eastern Europe was perhaps the most significant policy tool for advancing democratic reforms and human rights protection, and it seemed for a while that this would also extend its leverage into the Western Balkans and Turkey.

In the last decade, EU policy commitments and instruments have continued to develop at a formal level, even as international trends began to look less favourable for democracy. Governments agreed a set of Council Conclusions in 2009, which reiterated the commitment to the promotion and protection of human rights[299]. EU development cooperation became more political in its stated aims, with the European Commission's Agenda for Change placing support for democracy and human rights at the heart of development aid[300]. In 2012, the EU agreed a Strategic Framework and Action Plan on Human Rights and Democracy[301], building on the joint Communication issued by the Commission the year before[302]. Democracy support was also formally built into an array of external policy frameworks, such as the European Neighbourhood Policy[303] and the EU Consensus on Development[304]. From 2016, EU Delegations were obliged to report on Commission and Member State initiatives in support of democracy and human rights in their respective countries[305].

Although the 2016 Global Strategy centred mainly on security issues, it did formally confirm EU support for human rights and democratic norms around the world. EU foreign policy would aim to foster 'resilient states', based on a conviction that 'a resilient society featuring democracy, trust in institutions, and sustainable development lies at the heart of a resilient state'[306]. Concerned at a gathering authoritarian surge in many regions, European governments issued Council Conclusions in October 2019 with an

[299] Council of the European Union, 'Council conclusions on Human Rights and Democratisation in third countries', 2985th Foreign Affairs Council meeting, Brussels, 8 December 2009.
[300] European Commission, 'Increasing the Impact of EU Development Policy: An Agenda for Change', COM(2011) 637, 2011.
[301] Council of the European Union, 'EU Strategic Framework and Action Plan on Human Rights and Democracy', 11855/12, 25 June 2012.
[302] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and The Council. Human Rights and Democracy at the Heart of EU external actions- Towards More Effective Approach', 12 December 2011.
[303] European Commission and High Representative of The Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions. Review of the European Neighbourhood Policy', JOIN(2015), 18 November 2015.
[304] European Commission, 'European consensus on development', 2017.
[305] For more detail on these innovations, see F. Gomez, C. Muguruza and J. Wouters (eds.), *EU human rights and democratisation policies: achievements and challenges*, Routledge, London, 2018.
[306] European External Action Service (EEAS), 'A stronger Europe: a global strategy for the European Union's foreign and security policy', 2016.

upgraded commitment to democracy support[307]. In 2020, they adopted an Action Plan for Human Rights and Democracy 2020-2024 [308].

### 4.1.2 Digital elements in the policy framework

Alongside, and sometimes within the battery of, core external human rights and democracy strategies and instruments, the EU has incrementally accumulated commitments more specifically related to the repressive use of digital tools in third countries.

In 2011, the EU devised its first comprehensive instrument tailored specifically to digital threats to democracy, the so-called 'No Disconnect Strategy'. This was linked in part to the popular revolts of the Arab spring; while activists' use of social media revealed the positive democratic potential of digital technology, authoritarian regimes resorted to internet shutdowns and other restrictive moves in an attempt to neutralise the pro-democracy protests than ran through 2011 and 2012. As they did, EU concerns grew that this could jeopardise the Arab spring's democratic potential and it drew together various parts of its toolbox under the rubric of what it named the 'No Disconnect Strategy'[309].

The Strategy's strands included funding to help democratic activists build secure communications; training and capacity in cyber security for civil society organisations; and pressure on European companies to step back from abetting Arab regimes' digital crackdowns, with an attempt to build digital human rights issues into a widened concept of corporate social responsibility. The strategy promised to protect democratic activists and citizens from internet disruptions and surveillance from authoritarian regimes. It proposed funds for projects covering online privacy and security of people living in non-democratic regimes, for educating activists and raising their awareness of the risks involved with online communications, and for building cross-regional co-operation amongst activists to protect human rights[310]. One concern in the strategy was finding a way to get cyber protection to activists more quickly than allowed for by standard EU tenders and calls for proposals. Under the strategy, the EU also moved to prepare a European Capability for Situational Awareness that was designed to provide better information of digital abuses around the world.

While the strategy was an important step forward and innovative for its time, after its key driving force, Commissioner Kroes, retired, some of the momentum behind the No Disconnect Strategy dissipated. The Arab Spring's atrophy also undercut some of its rationale and the EU had to grapple with complex difficulties in continuing to support democratic reform in this context. At this stage, most Member State governments did not attach priority importance to digital repression elsewhere in the world; they and the top echelons of EU foreign and security policymaking had other geopolitical priorities that cut across the incipient rise in digital authoritarianism. The strategy was soon, in effect, broken up into different parts. While it did not survive in its original forms – like the European Capability for Situational Awareness concept, for example - the ideas it introduced became the basis for the raft of EU instruments that followed in subsequent years[311].

[307] Council of the European Union, 'Council Conclusions on Democracy', 12836/19, 2019.
[308] European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, 'EU Action Plan on Human Rights and Democracy 2020-2024', JOIN (2020)5, 23 March 2020.
[309] European Commission, 'Press release: Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally', 12 December 2011.
[310] European Commission Directorate-General for Communications Networks, Content and Technology, 'No Disconnect Strategy Workshop: European Capability for Situational Awareness (ECSA)', p. 1, 2012.
[311] Information in these two paragraphs draw on an interview with representative of an EU institution, 9 December 2020.

### 4.1.3 EU Human Rights Guidelines for Freedom of Expression Online and Offline

In 2014, EU Human Rights Guidelines for Freedom of Expression Online and Offline[312] committed the Union to push back against digital repression. These Guidelines represent a clear statement of intent and an essential part of the EU's toolbox. They are wide-ranging, but include several commitments relevant to this study. The guidelines stress that 'all human rights that exist offline must also be protected online, in particular the right to freedom of opinion and expression and the right to privacy.' These rights 'must be respected and protected equally online as well as offline'.

In terms of actions, the guidelines are largely about relatively imprecise and soft tools of persuasion, although they do go beyond those of other international organisations in their third-country funding elements. They are mostly couched in terms of promises that the EU will 'call on states', 'appeal to state authorities', 'encourage states', 'urge states', 'ask states for', 'advocate against restrictions', 'support actions and legislation by third countries', 'raise awareness', 'condemn abuses' and 'facilitate the exchange of experience and good practices'.

Most tangibly, the guidelines say that the EU will 'continue to provide journalists and other media actors, human rights defenders, political activists and other individuals with the technical tools and support they need in order to exercise their right to freedom of expression online as well as offline'. It will 'provide technical support to individuals on the ground to help counter online restrictions and abuses'. The EEAS and the European Commission 'will support the efforts of third countries to develop unhindered and safe access and use of the Internet in the context of ensuring openness and respect for human rights.'

Beyond such concrete funding pledges, the EU will raise restrictions against online freedoms in political dialogues with third countries. Delegations will monitor and report on developments relating to online freedoms around the world, often a difficult task in countries suffering from internet restrictions. The EU promised to 'encourage and facilitate' contacts with the CSO on these issues in partner countries. The EU will also monitor and increase its focus on online restrictions in candidate countries through pre-accession processes and mechanisms.

The guidelines contain some more strongly worded intimations at action, like demarches. These state: 'Abusive restrictions on freedom of expression and violence against journalists and other media actors should be taken into account by the EU when deciding on possible suspension of cooperation, notably as regards financial assistance'. Many, if not most, of these commitments are hedged with the caveat 'as appropriate', which might be read as diluting the EU's conviction in giving clear priority to this area of concern in its external actions.

### 4.1.4 Other instruments and initiatives

In recent years, the EU has introduced numerous cybersecurity instruments and initiatives aimed at countering disinformation and other influence operations emanating from third countries; as shown below, these have some points of overlap with the EU's external democracy support agenda.

The 2013 EU Cyber-security Strategy[313] was mainly framed around a state security narrative, but it also stressed that digital threats to global human rights were relevant to its mandate. The 2014 Council

[312] Council of the European Union, 'EU Human Rights Guidelines for Freedom of Expression Online and Offline', Foreign Affairs Council, 12 May 2014.
[313] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'Cybersecurity strategy of the European Union: an open, safe and secure cyberspace', JOIN(2013) 1, 7 February 2013.

Conclusions[314] on Internet Governance similarly stressed the importance of defending human rights from digital repression.

The new Action Plan for Human Rights and Democracy agreed in 2020 places much greater emphasis on the digital elements to EU external efforts than any previous policy instrument in this field, alongside the standard range of priorities like support for civil society, political parties, and human rights in multilateral forums.[315]

In a recent development, in December 2020, Commissioner Vera Jourova presented the European Democracy Action Plan (EDAP). This is not part of the EU's external toolbox in the same way as other instruments covered here, as it does not itself entail new funds or diplomatic resources. Yet, it is relevant to this study to the extent that it promises to join together efforts to protect digital rights within the EU with their promotion externally in third countries. The EDAP focuses on three issues: online disinformation, digital attacks on elections, and media pluralism. The EDAP is based on the premise that defending against attacks on elections in the EU and other powers' use of digital disinformation requires the source of these operations to be targeted within third counties. It points out that this strengthens the need for the EU to support human rights and democratic values internationally. This serves as an important policy reference point for efforts to mitigate digitally-driven authoritarianism globally, even if the EDAP does not in itself (yet) add concrete external funds or foreign policy instruments to the EU toolbox.[316]

Moving beyond this brief sketch of the overarching evolution of EU democracy and human rights commitments, the toolbox can be disaggregated into a number of quite distinctive parts. These include various forms of critical pressure; formal dialogues; funding mechanisms; and the EP's various instruments. The following sections examine their specific relevance to digital challenges.

## 4.2 Restrictive measures and conditionality

A first group of EU instruments aims to find ways to exert critical leverage over third countries to improve their democratic and human rights norms. These various instruments are about different forms of pressure over third countries. They have general relevance to human rights and democracy, but also more specific features related to the overtly repressive use of digital tools – they are pertinent, in this way, to a select part of the problematic trends described in Chapter 3, although less so to the more subtle forms of social control or advanced AI techniques.

### 4.2.1 Democracy and Human Rights Sanctions

The EU has increased its use of sanctions in recent years as its focus on economic statecraft has moved up several gears. It had more than 40 sets of restrictive measures in place at the end of the 2010s.[317] These are mostly restrictive measures targeted against individuals; some are country-based, while others are thematic, as described below. Most of its punitive measures have been related to conflict and security concerns, as in Afghanistan, Bosnia and Herzegovina, Iran, Mali, Russia, Somalia, South Sudan, Syria and Yemen. Where related to these kinds of conflicts and security concerns, EU restrictive measures are commonly adopted under the umbrella of sanctions agreed in the United Nations. These sanctions are not defined expressly or primarily as human rights or democracy measures, even though in practice they invariably punish human rights abusers involved in violence.

[314] General Secretariat of the Council of the European Union, 'Council conclusions on internet governance', 16200/14, 27 November 2014.
[315] European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, 'EU Action Plan on Human Rights and Democracy 2020-2024', JOIN (2020)5, 23 March 2020.
[316] Ibid.
[317] European Commission, 'The List of all EU sanctions'. See also S. Raine, 'Europe's Strategic Future: From Crisis to Coherence?', International Institute for Strategic Studies, London, 2019, p. 122.

Separately, the EU adopts its own autonomous sanctions. In recent years, the EU has applied such sanctions in relation to human rights abuses and democratic regression. Examples include Belarus, Myanmar, Iran, Venezuela and Zimbabwe. The EU's human rights and democracy sanctions have most commonly taken the form of asset freezes and travel bans targeted at a certain number of regime officials, rather than more sweeping measures against a country, per se. The EU generally seeks to retain strands of engagement alongside tightly delineated targeted measures against individuals.

Overall, the EU has generally been relatively sparing in its use of sanctions for democracy and human rights reasons. It has used sanctions often against relatively weak states and where strategic interests were less pressing. It has used restrictive measures in the most serious human rights cases, and it has targeted individuals rather than regime behaviour, as such. Even when the EU has imposed restrictive measures, it has invariably targeted fewer individuals, with softer restrictions and for shorter periods of time, than the U.S. measures in each case. In most cases, the EU has continued to deepen its relations with regimes engaged in digital repression.

EU sanctions could be said to be relevant to digital repression to the extent that the entities and individuals they target come from countries where online abuses have intensified. Digital concerns have been a part of several sanction regimes, including those applied in the cases of Belarus, Myanmar, Iran, Syria, and Venezuela. This was in the form of a listing criterion relating to the use of digital surveillance equipment and prohibitions on the export of monitoring equipment to them.

Still, digital repression has not itself been the main target of restrictive measures nor sufficient as a reason for imposing sanctions. There are many countries where digital abuses have worsened and yet the EU has sought to improve relations rather than sanction such repression; indeed, this is the most common dynamic in EU external action around the world. The EU has rarely sought to separate out digital problems from wider human rights and democracy challenges, as diplomats generally feel this would be somewhat artificial and difficult to do.[318] Its restrictive measures have been applied to cases where online abuses represent just one strand of a far bigger picture of deteriorating political conditions.

In December 2020, the EU adopted a new Global Human Rights Sanctions Regime. This came eight years after the United States introduced the so-called 'Magnitsky Act', named after the Russian human rights lawyer Sergei Magnitsky, who was killed in detention. While the new regime is a major step forward, it also exhibits limitations (an analysis of these is beyond this study's remit but can be found in other sources).[319] How far the new sanctions regime is relevant to digital repression is uncertain. The list of human rights abuses that fall within the mechanism's scope centres on core issues like torture, killings, violence, slavery, and genocide. The regime excludes corruption as a targetable offense, making it harder to seize kleptocrats' funds. However, it does include the freedoms of expression and association, which could prove relevant to regimes' use of digital tools for authoritarian repression (although probably not other elements of the trends outlined in Chapter 3).

Conversely, the EU may now use the new regime to focus more on sanctioning small groups of individuals for egregious rights abuses rather than the more structural and political problem of digitally driven repression. Moreover, the EU's use of its other sanction regimes in its responses to terrorism, digital attacks on Europe, and the use of chemical weapons could easily cut across the priority it gives to human rights and digital authoritarianism. Good and bad performers are different on these different issues; this means

[318] Interview with representative of an EU institution, 27 November 2020.
[319] R. Youngs, 'The EU's Global Human Rights Sanctions regime: Breakthrough or Distraction?', Carnegie Europe, December 2020.

that different sanction regimes could collide with each other and make it more difficult for policymakers to single out issues of digital rights abuses.

### 4.2.2 Cyber sanctions

More specifically related to the digital sphere, the EU has introduced a sanctions regime against individuals in third countries found guilty of cyberattacks.[320] In July 2020, the first measures were imposed against Russian, Chinese, and North Korean hackers and responsible entities. These sanctions are not directly targeted at digital repression within third-countries, and so their relevance to external human rights and democracy support is not obvious – at least, so far. They are designed to protect the EU itself from digital influence operations; that is, the kind of transnational dynamics outlined in foregoing chapters.

Still, in practice, these are measures against operators within the state apparatuses of regimes that are guilty of particularly far-reaching digital repression. The trolls and other operators in Russia and China penalised for influence operations against the EU – and those that the EU has sought to track more assiduously and effectively by building up its cyber capabilities – are of a piece with these regimes' digital repression of domestic populations. In this sense, these digital sanctions could be defined as indirect instruments for external human rights and democracy support. The use of these instruments could be widened in this direction, even if for now they are not currently framed in a way that is directly aimed at the global surge in digitally-driven authoritarianism.

The Commission has very loosely and speculatively floated the possibility of developing a sanctions regime specifically for disinformation as part of moves to implement the European Democracy Action Plan, although it is not yet clear whether this will proceed[321]. Whether Member States actually want to make this a top priority is not entirely clear, however. When discussing tougher sanctions and expediting the new cyber sanctions, most EU governments have been reluctant to let digital repression cut across other policy priorities. In a complex episode subject to much internal dispute, uncertainty, claim, and counter-claim, the press reported that the EU diluted its criticism of China's disinformation campaign during the early months of the COVID-19 pandemic. Stung by widespread criticism, at least some EU commissioners, officials, and leaders seemed to later toughen their position, becoming more critical towards China. The EU's criticism of Russia for COVID-related disinformation was more robust. [322]

### 4.2.3 Conditionality

The use of so-called 'human rights and democratic conditionality' involves exerting a softer and more subtle form of leverage than sanctions. This does not include legal restrictions or prohibitions, but decisions to hold back funding and/or trade preferences when governments infringe democratic norms or human rights. As with sanctions, the EU has not used such conditionality to such an extent that there is any strong overall correlation between countries' levels of democracy and EU aid and trade flows.

While the EU often wields a degree of democracy and human rights conditionality, most EU aid goes to non-democratic or partially authoritarian regimes[323]. This general observation applies, with some importance, to the more specific issue of digital repression. The EU often uses its other external funding for aims that sit uneasily with its supposed digital rights commitments. To give just one illustrative example,

[320] Council of the European Union, 'Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States', 7299/19, 14 May 2019.
[321] A. Brzozowski, 'Commission floats sanctions regime for disinformation offenders', *Euractive*, 3 December 2020.
[322] Financial Times, 'EU pressured to give results of leak probe on China disinformation', 21 June 2020.; The Guardian, 'EU says China behind huge wave of COVID-19 disinformation', 10 June 2020.; Reuters, 'EU's Borrell accuses Russia of spreading COVID-19 disinformation to sell its vaccine', 28 December 2020.
[323] K. Godfrey and R. Youngs, 'Towards a New EU Democracy Strategy', Carnegie Europe, 2019.

Chapter 2 identifies India as a state that has used a particularly wide and intrusive range of digital repression and social control mechanisms, and yet the EU has made notable efforts to upgrade its security cooperation with this country for broader strategic reasons. Similarly, China's even more egregious digital repression has not prevented the EU from deepening its commercial ties or signing a comprehensive agreement on investment with Beijing. Furthermore, in recent years there have been many EU aid projects across Africa and the Middle East, which train security and border guards in how to use invasive digital surveillance equipment, as they work with authoritarian regimes for a range of security objectives[324].

There is little evidence of the EU using conditionality specifically or explicitly as a response to digital repression or online distortion of democratic processes. The EU most commonly suspends aid for a short period of time following unfree and violent elections, or sometimes in response to very dramatic interruptions of democratic constitutional provisions. So far, political conditionality has not moulded itself to the more specific challenge of regimes using digital repression tools and tactics. In interviews carried out for this study, officials suggested that it would be difficult to separate out specific indicators for digital repression that could, in any primary operational sense, condition the level of overall aid flows to different countries – even if countries loosening restrictive laws could be given specific cooperation to help them do this. Certainly, the more subtle forms of social control, health system development, and AI techniques described previously in this report have not leant themselves readily, or in any tangible sense, to conditionality-based variations in EU levels of cooperation and engagement with third countries. The EU's monitoring and understanding of digital abuses around the world has improved significantly in the last several years, yet its tangible responses, beyond rhetorical criticism, have not evolved to anything like the same extent.

### 4.2.4 Restrictions on surveillance equipment

After a crucial and long-running debate that is directly and expressly relevant to the phenomenon of digital repression, in November 2020, trialogue talks resulted in agreeing text for a recast of the dual-use regulation that will tighten restrictions on sales from Europe of digital surveillance equipment to countries where human rights violations are taking place. It is not clear, however, that such restrictions will be severe enough to make these measures an effective part of the EU policy toolbox.

European companies making digital surveillance equipment have grown dramatically in recent years; companies from the EU are responsible for the second-highest earnings from the global market for such equipment[325]. In the early 2010s, some EU states pressed for digital equipment to be included under the multilateral Wassenaar Arrangement on export controls (The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies was established in 1996 and has 42 member states; it works towards 'promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies'[326]). From as early as 2014, the Commission called for autonomous EU export controls to be extended to digital surveillance equipment[327].

After several years of internal discussion on this issue, the Commission proposed a comprehensive dual-use regulation in 2016 to tighten controls on the export of potential harmful technology. The core notion was to give the EU the scope to apply autonomous measures beyond the multilateral Wassenaar Arrangement. At this stage, the proposals did not win widespread support among Member States. Member

[324] Privacy International, 'Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes', 10 November 2020.
[325] Amnesty International, 'Out of Control: Failing EU Laws for Digital Surveillance Export', 2020, p.11.
[326] For more detail, see www.wassenaar.org.
[327] B. Wagner, J. Bronowicka, C. Berger, T. Behrndt, 'Surveillance and censorship: the impact of digital technologies on human rights', European Parliament, 2015, from p. 27.

State governments were concerned about how the measures might prejudice security relations with many countries. They were also reluctant to forego lucrative surveillance technology contracts. A majority of Member States worked to dilute the Commission proposals and leave their digital elements relatively modest. For several years, several various Member States undercut the Commission's efforts to limit EU companies' exports of digital surveillance equipment likely to harm human rights[328].

Member States' opinions began to shift, however, as the scale of digital problems became apparent and also as the United States moved towards far stricter controls, putting pressure on European governments to tighten their own export controls. The use of surveillance against pro-democracy protestors in Hong Kong in 2020 shone a spotlight on digital repression. In this case, the EU did move to prevent companies providing surveillance equipment that could be used against democracy protestors[329]. In 2019, Member States reached an agreement in support of the Commission's proposals and more constructive negotiations on the details of a new regulation began with the EP playing a vital role as co-legislator.

The Recast Dual-Use Regulation strengthens human rights criteria and explicitly stipulates cyber-surveillance equipment as a dual-use good. Human rights violations are now a justifiable reason for placing controls on the export of such equipment. The regulation also adds some categories of cyber-surveillance equipment beyond those already covered by multilateral dual-use controls[330]. There is still much debate over important details within this regulation, particularly relating to exactly what kinds of equipment shall fall within its remit. Some Member States want a wider scope to include facial recognition technology and other innovations, while others have requested a narrower, more focused approach. Officials acknowledge that compromises have been made and that much will depend on the political will to take the regulation forward. The key factor will be how the EU assesses whether regimes are, in fact, using European technology for repressive ends, and whether such assessments should be made public[331].

## 4.3 Dialogues and multilateral engagement

### 4.3.1 Human rights dialogues

The EU often stresses the need to exert pressure through political dialogue. It currently has 45 human rights dialogues with partner countries. Formally structured dialogue is a vital part of the EU's human rights and democracy toolbox. Officials interviewed for this report generally acknowledged that the EU's human rights dialogues were relatively slow to hone-in on digital concerns, but stressed that they have begun to do so – knowledge and appreciation of the scale of this problem has gradually caught up with trends around the world.

The human rights dialogues that have in recent years come to include a focus on digital rights include those with China, Ethiopia, the Gulf states, and Uzbekistan. In 2021, digital rights and repression will be on the agenda of all EU human rights dialogues. Still, some states have effectively resisted even discussing digital concerns within these dialogues; Russia is a prime example of this[332].

The EU approaches its dialogue on digital issues mainly through a freedom of expression prism, although it has begun to include a focus on surveillance and privacy rights. The EU most commonly uses its formal dialogue forums to raise the cases of individuals suffering human rights abuses, including through digital means. The EU has increasingly focused on regimes' online smear campaigns and repression against

[328] Interview with key informant interviewee 01, under full anonymity, 24 November 2020.
[329] Politico, 'EU to limit export of 'sensitive' tech in response to Hong Kong security law', 28 July 2020.
[330] European Parliamentary Research Service, 'Review of dual-use export controls', January 2021.
[331] Interview with key informant interviewee 01, under full anonymity, 24 November 2020; see also Amnesty International, 'Out of Control: Failing EU Laws for Digital Surveillance Export', London, 2020, p. 12; G. Gressel. 'Protecting Europe against hybrid threats', European Council on Foreign Relations, London, 2019, p. 114.
[332] Interview with representatives of the EEAS, 2 December 2020.

opposition leaders and democracy activists. Again, it has also sought to broaden this traditional approach out to address more structural rules that relate to digital rights in third countries.

It is within such external dialogues that the EU has also cautiously begun to expand its digital strategies to address some of the wider array of concerns and controls outlined in Chapter 3. Policymakers are increasingly pushing back within dialogues on states' use of facial recognition and bio-surveillance, and their use of more subtle techniques, like slowing down connections rather than complete internet shutdowns. They concur that this is where challenges are likely to become pressing in the future, and that much deeper consideration is needed of how the EU can move beyond raising general concerns to making decisions with concrete impact in its foreign policies. Policymakers admit that the EU is still in the early stages of dealing with the international dimensions of AI adoption, which are quite different from the sensitive issues of rights abuses associated with this technology[333].

In relation to COVID-19 health controls, the EU has increasingly sought to internationalise its focus on data privacy. The EU is now exerting pressure, in both its bilateral dialogues and its interactions with the WHO, to begin discussions on how broader rights issues might be considered in overarching public health diplomacy and policymakers. This is about offering expertise on norm-setting for privacy, but also looking at forms of pressure as and when regimes use COVID-19 to tighten digital control more broadly over their societies. The February 2021 Council conclusions promising a 'human rights-based recovery' from COVID-19 included references to online rights issues, and might serve to help the EU's incipient efforts to widen the digital components of its human rights dialogues.[334] Still, beyond fairly tentative dialogue, most states in the EU are reluctant to use aid that is being disbursed as a humanitarian response to COVID-19 for leverage over a political issue like digital repression.

### 4.3.2 Multilateral dialogue and engagement

Alongside its human rights dialogues with particular third countries or regional groupings, the EU has also increasingly prioritised wider multilateral dialogue for its digital agenda. The EU has promised to strengthen the UN's focus on and defence of freedom of opinion and expression online, including through the mandate of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, and by cooperating closely with the special rapporteurs with related mandates from the AU, OAS, OSCE and OIC. It has advocated the inclusion of these issues within the Human Rights Council's Universal Periodic Review process and has engaged with the Office of the United Nations High Commissioner for Human Rights (OHCHR) in relation to online protections[335].

The EU has supported several more specific multilateral forums that are aimed at fostering dialogue on online human rights issues. It has, for example, backed efforts to develop multilateral internet governance forums that protect online rights, like the Internet Governance Forum (IGF)[336] and the Freedom Online Coalition (FOC)[337]. President Emmanuel Macron's 2018 Paris Call for Trust and Security in Cyberspace stressed that offline rights must also be protected online; it connects 64 states and technology companies with a loose intent to take future action[338]. The Commission and High Representative's proposal for a 'New EU-US agenda for global change' presented in December 2020 includes the suggestion that the EU and US

[333] Interview with a representative of EU institution, 12 March 2021.
[334] Council of the European Union, 'COVID-19: Council adopts conclusions on human rights-based recovery', 22 February 2021.
[335] Council of the European Union, 'EU Human Rights Guidelines on Freedom of Expression Online and Offline', Foreign Affairs Council, 12 May 2014.
[336] See Internet Governance Forum, available at www.intgovforum.org.
[337] See Freedom Online Coalition, available at www.freedomonlinecoalition.com.
[338] S. Garside, 'Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom', College of Europe EU Diplomacy paper 01, 2020, p.30.

set up a 'Transatlantic Artificial Intelligence Agreement to set a blueprint for regional and global standards aligned with our values'.[339]

Most of these forums and initiatives tend to make statements about the need for generic standards, rather than being mobilised in relation to specific cases of rights abuses. It is difficult to identify cases where such dialogue forums have leveraged firm pressure on governments to step back from authoritarian behaviour generally, or the use of digital tools for non-democratic ends more specifically. The EU has struggled to move either the IGF or the FOC beyond dialogue on general standards to become forums that are directly relevant to policy in relation to concrete instances of digital repression[340].

As reported in interviews carried out as part of this study, some policy makers see the current raft of EU measures aimed primarily at regulating platforms' operations within the Union - such as the Digital Markets Act, Digital Services Act, European Democracy Action Plan and upcoming AI instrument - as tools to be raised more purposively in multilateral human rights dialogues. It is recognised, however, that these generally have a tangential rather than direct relevance to the politics of core global human rights challenges in specific countries. There appears to be an emerging effort to deploy these kinds of new measures to buttress norm-setting at the global level, using their impact on digital questions inside the EU as templates which the EU can use to encourage third countries to implement reforms. Still, the EU is only just beginning to tentatively include discussions on potentially more concrete uses of such instruments for rights-related digital norms in third countries in its human rights dialogues at the global level – a potential step forward, but not one with a tangible impact on the foreign policy toolbox yet. The EU is especially supportive of a UN 'tech envoy' with a strong mandate to give these efforts greater impetus.

### 4.3.3 Engaging the private sector

The EU has worked with the UN to engage the private sector in dialogue about due diligence on human rights. The EU has supported the United Nations Guiding Principles on Business and Human Rights, and worked with the UN to bring digital concerns into national action plans under the rubric of these principles. The Commission has also developed guidance for tech companies based on the UN principles[341]. Still, there are concerns among policymakers that the UN principles are not highly operationally relevant for day-to-day foreign policy challenges and crises, and are not yet an avenue of great potential for a strong approach to tackling the high-level geopolitical tensions involved in digital rights issues. It is also felt that norm-setting related to business and human rights guidelines has been pertinent mainly to the extractive industries sector rather than digital companies, while the new EU human rights due diligence instrument is similarly expected not to be centrally tailored to digital issues[342].

In its dialogues and outreach, the EU has increasingly sought to persuade private companies to conduct due diligence to ensure their digital operations do not have negative human rights impacts. This is not a new effort, but it is one that has expanded to cover the private sector's complicity in online right abuses and democratic restrictions. The aim has been to encourage companies to undertake human rights impact assessments and to expand these to digital operations. Several social platforms have commissioned consultancy companies to undertake such assessments.[343] This is not directly part of the EU toolbox, as these are not instruments directly under the EU's control (such as decisions on funding or sanctions), but

[339] Commission and High Representative, 'A new EU-US agenda for global change', JOIN(2020)22, p.6
[340] Garside, p.11
[341] Shift and the Institute for Human Rights and Business, 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', European Commission.
[342] Interview with representative of an EU institution, 27 November 2020.
[343] Business and Human Rights Resource Centre, 'Human rights due diligence within the tech sector: developments and challenges', 1 December 2020.

the guidance does represent a pertinent means of soft persuasion over the private sector. Those Member States that are part of the FOC have also used this forum as an avenue for dialogue with private sector actors on internet freedoms. At each of these levels, the focus has been on positive encouragement, and there has been little EU appetite to wield punitive sanctions against companies attached to mandatory due diligence requirements[344].

Policymakers acknowledge that engagement with the private sector is one of the areas where progress has been most modest so far**.** The EU has gradually begun to redress this situation, although diplomats recognise it is an area that still lags behind the focus on state-to-state relations or the more standard diplomatic channels of foreign policy. The EU has started to arrange several NGO forums with private sector involvement, seeking to position itself as a 'bridge-builder' between civil society and private companies. A growing number of such dialogues are focusing on human rights CSOs working with companies to achieve stronger protection of safe online spaces for human rights defenders in autocratic states. Many decision makers believe that the EU is well-positioned to foster this kind of dialogue-based approach with human rights CSOs and businesses, rather than favouring highly punitive approaches, for instance on due diligence (even though on this last issue, some degree of support is growing across different EU institutions and member states for firmer action). Incipient dialogues tend to include social media platforms and aim to get them working with human rights groups. They have not yet aimed to apply concrete pressure on IT companies to actively resist internet shutdowns[345]. Still, notwithstanding these advances, the EU's contacts, dialogues and coordination with the private sector have so far focused overwhelmingly on internet regulations within Europe itself**.** Our interviews revealed that the EU has not yet reached out in any concerted way to tech companies in relation to the rights concerns outlined in Chapter 3. There is concern that the spill-over of internal policies into external EU policies has been largely negative; this is because national Member State laws, such as Germany's NetzDG, have been used by regimes around the world as a template for their own restrictive rules on the internet. Private sector representatives highlight that EU policymakers have been interested in working together to prevent influence operations from third countries having an impact inside Europe, but not to deal with the effects of digital repression within third countries themselves.

As revealed during the interviews, private sector (EU-based and US platform) representatives support the EU's efforts to develop standards at the multilateral level, but are also concerned that the EU can rather overstate the potential of such guidelines and generic principles. These do not deal with immediate compliance challenges and, in relation to these platforms, some companies do not feel there has been adequate EU diplomatic support, dialogue, or action – often for cross-cutting geopolitical reasons. Since the EU has sought to bring stakeholders together from the private sector, civil society, and governments to coordinate domestic policies, as mentioned earlier, this is gradually being replicated at a broader, international level. One case of untapped potential relates to a possible internationalisation of the Rapid Alert System on which the EU and platforms cooperated for the EU elections in 2019. This kind of coordination is still sporadic in relation to digital manipulation in elections outside Europe, occurring in some countries but not in others, and is not subject to consistent global rules[346].

## 4.4 Funding

The EU has gradually increased the funds it allocates directly to democracy and human rights policies. It funds such projects through multiple instruments and budget lines. This makes it impossible to put a single, precise figure on the magnitude of the funding. It is certainly the case, however, that these funds have gained importance within the EU's overall democracy and human rights toolbox. The EU is currently

[344] Interview with representative of an EU institution, 27 November 2020.
[345] Interview with representative of an EU institution, 27 November 2020.
[346] Interview with private sector representative, 20 January 2021.

in the midst of restructuring its funding instruments in ways that will have implications for human rights and democracy generally, and for projects on digital issues more specifically.

### 4.4.1 European Instrument for Democracy and Human Rights

The budget line that is specifically dedicated to democracy and human rights funding, the European Instrument for Democracy and Human Rights (EIDHR), has amounted to just over EUR 160 million each year since 2014, with a total EUR 1.3 billion for the 2014-2020 budget period. Around 90% of EIDHR funding is allocated for civil society[347]. The EIDHR is a distinctive part of the EU toolbox to the extent that it funds civil society actors without needed formal governmental consent. It can also now also fund non-registered entities, allowing funds to go to a wider range of civic actors, such as those involved in pro-democracy social movements, that can make a significant difference where popular mobilisations have built up strong momentum.

The EIDHR funds the EU's election observation operations. The EU now deploys some eight to ten election observation missions (EOMs) a year, and an increasing number of electoral follow-up missions (EFMs)[348]. Of relevance to this report, the EU has recently incorporated a focus on online distortions of election processes in its electoral missions. It did so first in 2018 in Kenya and then in Sri Lanka. The digital remit then expanded and is now formally a part of all EOMs, as well as the electoral expert missions dispatched to more difficult cases where full EOMs are not possible. The EU has worked with the United Nations to develop guidelines on the use of digital technology in elections, with a view to incorporating these into its own missions.

Work on this emerging area of action has been somewhat set back by the COVID-19 pandemic. Election delays and logistical constraints meant that only three EOMs were deployed in 2020 – to Ghana, Peru, and Guyana. Nevertheless, the new Action Plan for Human Rights and Democracy identifies the digital threats to free and fair elections as a top priority for EU external action over the next several years. This action is set to include more rigorous EU monitoring of online activity and tactics during election campaigns, but also more support to build the capacities of local civil society organisations and independent electoral commissions in digital techniques. Officials acknowledge that the main challenge will be to move from a reactive stance of identifying and responding to instances of online electoral manipulation, towards a more pre-emptive policy of preventing such problems emerging well before campaigns begin[349].

While the EIDHR is the instrument most directly pertinent to this study, it is important not to overlook the sizeable amounts of funding the EU allocates for democracy and human rights from a rage of other geographic and thematic aid budgets. These have included the European Neighbourhood Instrument, the Development Cooperation Instrument, the Instrument of Pre-Accession Assistance, the Instrument contributing to Peace and Security, and various humanitarian aid budget lines. Funding for digital actions has not been an especially high priority in the democracy and human rights initiatives supported under these instruments, but the initiatives have been sources of some additional funds for these issues. Under these, the EU has funded many indirect digital empowerment initiatives that are less overtly political, such as its Digital4Development initiative. The new Neighbourhood, Development, and International Cooperation Instrument (NDICI) introduced under the 2021–2027 Multiannual Financial Framework will combine many of these different sources as a new umbrella framework for the digital elements of democracy and human rights support. With negotiations ongoing at the time of writing, it remains to be seen to what extent the NDICI will prioritise a new round of digital rights initiatives.

[347] Ken Godfrey, Richard Youngs. 'Toward a New EU Democracy Strategy', Carnegie Europe, 17 September 2019.
[348] Ken Godfrey, Richard Youngs, 'Toward a New EU Democracy Strategy', Working Paper, Carnegie Endowment for International Peace, p. 8, September 2019.
[349] These two paragraphs on EOMs draw from an interview with key informant interviewee 02, under full anonymity, 26 November 2020.

From this plethora of different instruments, the EU has focused on several main themes that relate specifically to the challenge of digitally-driven authoritarianism. These are discussed below.

### 4.4.2 Media pluralism

Relevant to the digital sphere, media pluralism has increasingly become a priority in repressive environments, and also in countries of conflict, where regimes often use the media to fan the flames of polarisation. This has routinely been framed as part of the EU's efforts to contain and pushback against non-democratic digital influences. The EIDHR launched a global call on digital activism in 2018, and has identified media freedoms and gender issues as particular priorities for 2019 and beyond. This priority is evident in calls for proposals at the headquarters level, in Delegations' funding priorities, and in the training currently provided for delegation staff to help them include media pluralism in programming.

European support for media freedom has gained extra momentum from a large-scale Media4Democracy project, allocated EUR 4.3 million in 2017, that focuses on the growing threat to freedom of expression both online and offline. The Media4Democracy project supports EU Delegations to advance several key priorities: combating violence and threats to online freedom of expression; promoting laws and practices that protect freedom of expression; promoting media freedom and pluralism and discouraging interference with impartial and critical reporting; promoting and respecting human rights in cyberspace; and promoting legal amendments and practices to strengthen data protection and privacy. The Commission reports that this initiative has generated an overall increase in Delegations' support for freedom of expression and medial pluralism programmes in the last four years[350].

### 4.4.3 Civil society and digital activism

The EU's generic focus on civil society support has intensified. Many EU Delegations have agreed on civil society roadmaps. The Commission's Supporting Democracy initiative provided just under EUR 5 million over three years, sending experts to work with civil society actors and EU Delegations[351]. Through its more flexible funding, the EU has continued to fund some civil society actors even in tough circumstances, such as in Azerbaijan, Belarus, Egypt, and Zimbabwe[352]. This is germane for this report because these are the kinds of states most seriously affected by digital repression. In these contexts, the EU has begun to work harder to enhance societies' general civic capacity in order to neuter and off-set regimes' digital tactics. Still, in many of the states identified in Chapter 2 suffering serious digital repression, like China, Iran and Russia, the EU has struggled to keep any significant amounts of independent civil society support going.

Within this broad category of civil society support, in the last several years the EU has begun to focus more on the specific strand of digital activism. EU support for digital civic initiatives has increased significantly in recent years and has become one of the leading edges of the Union's efforts to counter digitally-driven authoritarian influences. In 2018, the EU ran a CivicTech4Democracy initiative and launched a new EUR 5 million call to support civic activism through digital technologies — "a new priority reflecting the emerging problems associated with the online sphere"[353]. In 2020, the annual, EU-funded NGO Forum was focused on digital challenges to human rights as its central theme. Delegations in Israel and Liberia launched calls on digital democracy in 2020.

[350] Online consultation with representative of EU institution, 29 January 2021.
[351] Ken Godfrey, Richard Youngs, 'Toward a New EU Democracy Strategy', Working Paper, p. 8,
[352] European Partnership for Democracy, 'Louder than words? Connecting the dots of European democracy support', Brussels: EPD, 2019, p. 118; B. von Ow-Freytag, 'Filling the void: why the EU must step up support to Russian civil society', Martens Centre for European Studies, 2018, pp. 17-18.
[353] Ken Godfrey, Richard Youngs, 'Toward a New EU Democracy Strategy', Working Paper, p. 8.

**Box 10: EU toolbox on the ground: Myanmar**

Even as Myanmar embarked on a tentative political opening from 2012, problems worsened in the digital space. Although Myanmar is a poor country, internet penetration is high, specifically through Facebook. All phones come with Facebook already installed. For several years, the social media space has been used for hate speech and disinformation against minorities, often with at least tacit support from the military. After the military resumed full political control on 1 February 2021, it tightened online restrictions dramatically through a new cybersecurity law, and utilised tactics involving internet shutdowns and severe limitations on freedom of speech.

In recent years, the EU has increased its range of engagement with and in Myanmar. It allocated EUR 600 million in aid under the 2014–2020 budget. The EU has used this budget to fund a rapidly expanding civil society, including for political projects on elections and human rights with digital dimensions. Under a EUR 10 million programme on the elections, the EU supported efforts to increase online transparency around the candidates and their programmes as a way of pushing back against harmful apps. Another programme worth just under EUR 1 million worked to build the capacity of human rights defenders and marginalised groups, including through digital tools and techniques. At the end of 2019, the EIDHR began a EUR 1.8 million initiative to boost online protection for journalists in Myanmar.

At the diplomatic level, the EU has also continued to apply pressure through regular UN Human Rights Council resolutions and through restrictive measures: these have included an arms embargo (that covers dual-use goods and telecommunications equipment), asset freezes, and travel bans on around 40 regime individuals implicated in human rights abuses. The EU has also used the human rights dialogue to try to persuade the regime to change or remove restrictive digital laws. In 2020, the EU decided against removing GSP trade preferences as a means of leverage; the process of 'enhanced engagement' raised gross human rights and labour rights violations, although it did not identify digital restrictions as such[354]. The military's move in 2021 to reassume direct, fully autocratic control revealed the limitations of these various strands of engagement and left the future of EU projects on the ground uncertain.

### 4.4.4 Protecting activists from repression

Arguably most relevant to this report's remit is that more of the EU's funding now goes directly to protecting activists from state repression. Increasingly, "EU democracy support has shifted towards pushing back against negative trends like the shrinking space for civil society, disinformation, and attacks on electoral integrity"[355]. This funding has evolved in response to what Chapter 3 refers to as the 'next generation toolkit' of digital control. The EIDHR's emergency fund for human rights defenders can directly channel funds at speed when defenders face a moment of acute risk[356].

The EIDHR also funds a human rights defenders' protection mechanism, known as Protectdefenders.eu. ProtectDefenders.eu was set up in 2015 in order to provide a more comprehensive direct support mechanism for human rights defenders. It includes training on digital security for online activists, as well as temporary relocation and support for judicial procedures. Under this project, a consortium of 12 international NGOs provides emergency grants for relocation, individual security, and legal support. By early 2019, Protectdefenders.eu had provided over 1,000 emergency grants, training for 5,000 at-risk human rights defenders, and other support for just over 10,000 human rights defenders[357]. The EU has recently extended the contract until 2022 for the amount of EUR 10 million. The extent of digital protection,

[354] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Staff Working Document. Report on EU Enhanced Engagement with three Everything But Arms beneficiary countries: Bangladesh, Cambodia and Myanmar', SWD(2020) 19, 10 February 2020.
[355] Ken Godfrey, Richard Youngs, 'Toward a New EU Democracy Strategy', Working Paper, p. 9.
[356] Ibid.
[357] Ibid.

equipment, and training provided under the EU's various emergency grants has increased significantly in recent years. It is set to rise further as a priority under (the fourth pillar) the new Action Plan for Human Rights and Democracy from 2020 onwards. The Commission has encouraged Delegations to fund digital initiatives as a horizontal priority under human rights and democracy funding as a whole (especially the thematic programme that will secede the EIDHR) and to increase the scale of digital training for human rights defenders and journalists[358].

### 4.4.5 European Endowment for Democracy

Finally, one additional actor warrants mention. In 2013, a novel addition to European democracy funding began work: the European Endowment for Democracy (EED). The EED functions outside the formal EU institutional structures, although it is funded by the Commission and Member States. Since 2013, the EED has funded over 1,000 projects, worth more than EUR 50 million. 23 Member States have contributed funds. Initially, it worked only in European Neighbourhood Policy states, but in the latter part of the decade it has expanded to Russia, Turkey, and the Balkans. The EED's budget is still relatively small, at under EUR 20 million per year, but the organisation has established a high profile within European democracy support[359].

The EED follows 'an unconventional approach to democracy support' designed to fund democratic activists that do not receive help from other donors. It has flexible administrative rules that make it easier to support small, informal, or non-registered organisations; or even individuals. It funds new types of activism. The EED has a particularly strong focus on citizen journalists and grassroots organisations working to pushback against digital repression; digital literacy; alternative content generation; capacity-building for local digital initiatives; digital security for activists; and tailored protection for individual bloggers attacked by regimes[360].

**Box 11: EU toolbox on the ground: Kyrgyzstan**

On the ground in individual countries, EU diplomats face the challenge of dealing with digital and human rights issues as part of a wider ranging agenda. A case like Kyrgyzstan shows how, in practice, different parts of the EU toolbox interact and overlap with each other. This is a country where the digital agenda is relatively new for the EU and is just beginning to gather momentum, but where it has clearly grown in importance in recent years. The country is an example of a hybrid regime with some reformist elements, but an overarching trend of democratic backsliding. Neighbouring powers like China and Russia are distorting discourses and communication on the internet, but also some internal actors. Within this context, the EU has built digital components into most of its policy instruments. In terms of funding, the Media4democracy initiative has paid for civil society training. The EU has supported a EUR 21 million programme for digitalisation that is not specifically concerned with human rights, but includes some policy dialogue on rights standards. Digital concerns have become more of a priority within the EU's human rights dialogue; the EU teamed up with the UN to convince the government to pull back from a number of restrictive digital laws. The EU is also providing additional support to human rights defenders hit by digital attacks. It is building digital issues into a new, enhanced cooperation agreement set to come into effect next year, some focusing on online rights. It seeks to use the leverage of GSP-plus for the same aim. New post-2020 aid will include more work on digitalisation. The EU is beginning to develop all of these means of leverage, even though digital restrictions cannot yet be defined as one of the highest priorities. This case shows that on the ground, the digital element is one issue nested within a range of other political trends, and so it cannot be separated from these. The EU has deployed a combination of dialogue, funding, and pressure, grappling with the challenge of a context that allows some cooperation on digital tools, but where political trends continue in a negative direction despite the EU's upgraded efforts[361].

[358] Online consultation with representative of EU institution, 29 January 2021.
[359] European Endowment for Democracy (EED), 'Annual Report 2018: Supporting People Striving for Democracy', Brussels.
[360] Interview with a representative of the European Endowment for Democracy, 22 December 2020.
[361] This box draws from an interview with a representative of EU institution, 15 December 2020.

## 4.5 Overlaps with cyber-security and influence operations

The EU has developed a cluster of instruments in recent years that aim to strengthen the Union's ability to withstand various types of digital influence operations from third countries. This is a different agenda to support for human rights and democracy within third countries, which this report covers. Nevertheless, these two agendas have begun to overlap in places. A number of the new and emerging instruments in this area have begun to develop in a way that are relevant, at last at the margins, to this report's subject matter.

### 4.5.1 Stratcom

One very politically driven area of external funding activity has been carried out under the so-called Stratcom initiative, set up in 2015 by the External Action Service. With a very specific remit to counter Russian disinformation in the countries of Eastern Europe, the initiative worked to correct Russian disinformation and contribute to spreading good news stories about the EU in these countries. In this sense, the initiative has indirect relevance to this report's concern with digitally-driven repression in third countries. Stratcom was mobilised as a tool mainly to protect against disinformation within the EU and some non-EU Eastern Partnership states; it followed a security agenda, rather than aiming directly at human rights and democracy within the source countries of disinformation.

Still, the lines between these two agendas have been somewhat blurred. Stratcom's budget increased from EUR 1.1 million in 2018 to 5 million in 2019, and its remit was extended into the Balkans, North Africa, and the Middle East. Of direct relevance to this report, Stratcom operations in the south and the Balkans focus more on building local capacities to resist digital distortions to democratic processes and disinformation, in particular, than they have done in the east[362].

### 4.5.2 Cyber funding

In recent years, the EU put in place a large number of initiatives in the realm of cybersecurity. While these are designed to protect the EU's security from outside influence operations, a number of the new initiatives in this field have taken on at least some elements related to digital repression in third countries.

An initial EU Cybersecurity Strategy in 2013 was designed mainly to draw together the large number of fragmented areas of cybersecurity work in the EU, and better connect these to foreign policy. The Cybersecurity Emergency Response Team initiative was one of the largest projects funded under PESCO, while the European Cybersecurity Research and Competence Centre also gained influence. In 2017, the EU introduced the Cyber Diplomacy Toolbox. The issue was ostensibly mainstreamed into core defence policy through the 2014 Cyber Defence Policy Framework; this was updated and significantly expanded in 2018. Overall EU spending on cybersecurity increased exponentially, equating to billions by the end of the 2010s[363].

The EU Agency for Network Information Security (ENISA) morphed into a more institutionalised Agency for Cybersecurity, gaining powers and resources. In 2019, its budget doubled from around EUR 10 million to over EUR 20 million per year. The EU agreed a framework for a Joint EU Diplomatic Response to Malicious Cyber Activities. By 2019, cybersecurity accounted for half the workload of the Security Union[364]. The EU introduced cybersecurity dialogues into all of its main strategic partnerships and, in 2018, the High Representative convened a Global Tech Panel to examine the geostrategic implications of digital technology.

[362] Interview with representatives of EU institution, 27 November 2020.
[363] European Court of Auditors, 'Challenges to effective EU cybersecurity policy', Briefing paper, 2019.
[364] C. Mortera-Martinez, 'The EU's security union: a bill of health', CER, London, 21 June 2019. p.6.

It also set up a hybrid fusion cell and the European Centre of Excellence for Countering Hybrid Threats; agreed an action plan against disinformation; set up a 24/7 rapid alert system for Member States to notify of foreign disinformation campaigns; and got the major online platforms to sign a code of practice to cooperate on tackling disinformation. G7 leaders agreed to the so-called Charlevoix Commitment on Defending Democracy from Foreign Threats, committing to take concerted action to respond to outside threats to democratic elections.

Concerns around cyberattacks within the EU led to the allocation of funds for digital security initiatives in third countries, as a way of boosting their cyber resilience. Under the Instrument contributing to Stability and Peace, the EU is funding an increasing number of cybersecurity projects in other countries. While cyber funding has been primarily aimed at boosting cybersecurity capabilities within the EU, its external component has begun to expand[365]. This strand of policy is mentioned here because it is becoming an increasingly high priority for the EU; it has yet to incorporate any significant funding directly targeted at digital authoritarianism as such, although these capabilities could *de facto* prove highly useful in protecting civil society activists from attacks.

## 4.6 EP instruments and contributions

Through its Democracy Support and Election Coordination Group, the EP increased its work from 2014, mainly in the form of election observation and exchanges with other parliaments. Its activities include actions around the Sakharov prize, concrete capacity building, mediation, and support to human rights defenders and journalists. Some of these tools are relevant to new challenges in the digital sphere. The group lists countering fake news and supporting media pluralism among its priorities[366]. Its 2020 work programme does not foreground digital issues. Rather, it lays out the geographical priorities for its fact-finding missions and (pre- and post-) electoral dialogues, and for its large number of training, young leaders, fellowship, and human-rights related awards programmes. Still, it contains one highly significant mention of digital issues; the EP offered to co-host a meeting with the EEAS to support the latter's efforts to develop a 'declaration of principles for international election observation' that would include digital technology concerns[367].

More broadly, the EP has worked to raise the profile of several areas of digital issues and their links with human rights and democracy. In 2012, the EP passed a resolution entitled 'Digital Freedom Strategy in EU Foreign Policy' that urged the EU to place higher priority on defending 'digital freedoms', in particular within its development and other external funding programmes[368]. In 2015, it passed a resolution on 'Human rights and technology: The impact of intrusion and surveillance systems on human rights in third countries'. This focused primarily on concerns that the EU had failed to prevent European companies from supplying digital surveillance equipment to third countries that do not have rigorous human rights assessments. It also called for a number of concrete steps relating to the external promotion of digital rights. These included a 'human rights and technology fund' to be created under the EIDHR; new clauses to be included in all trade agreements referring specifically to the need to respect 'digital freedoms' and unhindered access to the internet; and a ban on companies failing to apply the digital due diligence elements of the UN Guiding Principles on Business and Human Rights from EU public procurement calls[369]. The interviewees for this study concurred that these EP resolutions have played a role in pushing the Commission and the Council to take action.

[365] G. Christou, 'Cybersecurity in the European Union: resilience and adaptability in governance', London, Palgrave, 2015.
[366] Democracy Support and Election Coordination Group.
[367] European Parliament Democracy Support and Election Coordination Group, 'Annual Work Programme 2020', 2020.
[368] European Parliament, 'Resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy', 2012/2094(INI), 11 December 2012.
[369] European Parliament, 'Resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries', 2014/2232(INI), 2015.

In the last several years, the EP has played a prominent role as co-legislator in relation to tightening export controls on dual-use surveillance equipment in line with the Commission's Recast Dual-Use Regulation. The DROI Subcommittee on Human Rights heard evidence in 2020 on COVID-19 related disinformation. The European Parliament has put in place a special committee on 'Foreign Interference in all Democratic Processes in the European Union including Disinformation'. While this is focused on policy concerns within the EU, its Rapporteur's first working documents make several references to the need to connect this concern with more active external action directed at digital abuses[370].

## 4.7 Conclusions - assessment of the toolbox's evolution

The EP's 2015 study, mentioned above, was not a detailed study of all elements of the EU toolbox, or specifically of the external dimension of digital rights issues, but it did suggest some general steps forward. These have proven highly relevant to subsequent policy developments, as the EU has moved to take on board nearly all of the report's main suggestions, namely: to 'encourage' other countries to respect digital freedoms; to build institutional knowledge on such issues; to bring digital issues into external dialogues (singling out Latin America in this regard); to make cyber-security more about rights and less about purely military-type security approaches; to support online protections for citizens outside of Europe; and to push for more UN work on digital privacy[371]. As this chapter has demonstrated, the EU's policy toolbox today reflects all of these ideas to a far greater extent than was the case before 2015. However, in the last several years, more specific issues have arisen in the EU's deployment of its toolbox that raise further challenges for the EU to address and continue improving its policy instruments. New concerns have arisen over the effectiveness, comprehensiveness, and efficiency of the EU toolbox, while various thematic dilemmas have become more acute:

**Effectiveness:** In recent years, the EU has retained – and even widened – its toolbox for human rights and democracy support against an extremely challenging global backdrop. Yet, the challenge of digitally-led authoritarianism has continued to deepen. As a result, the EU will need to look for ways to continue fine-tuning and adding to this toolbox. While the EU's general approach to human rights and democracy has sharpened in some notable ways, it is more difficult to conclude that its toolbox is fully attuned to the specific features of digital repression and contemporary democratic backsliding.

The EU's direct financial support has had a very clear, tangible impact on protecting many individual civil society activists from repression. Its broader funding initiatives aimed at enhancing the positive digital capacities of civil society have been useful in laying the groundwork for pushing back against digital repression, but the impact here is almost impossible to quantify with any precision. The EU's diplomatic pressure, dialogues, and attempts to build effective international standards are areas where the interviewees in this study felt that the EU's effectiveness is the hardest to pin down, in terms of an identifiable impact on the regimes' immediate political actions. While EU policies have improved, the desired results have not always been forthcoming, as regime attacks on democratic freedoms and human rights have become stronger and more far-reaching.

**Comprehensiveness:** The EU's toolbox has become more comprehensive in the last several years, as the EU has added a number of different strands to its efforts against digital authoritarianism. Digital rights issues have been incorporated, to some extent, into EU restrictive measures. Funding has increased for digital elements of external human rights and democracy. Online threats to democracy have become a staple of EU dialogues with third countries and within multilateral fora. EU cybersecurity cooperation has

[370] S. Kalniete, 'Working document on the state of foreign interference in the European Union, including disinformation', Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, 17 December 2020.
[371] B. Wagnar et al, 'Surveillance and censorship: the impact of technologies on human rights', EP Directorate-General for External Policies, 2015.

begun to adopt more of a rights-centred approach. Alongside focusing on regimes' repressive actions, the EU has also moved to limit European companies' involvement in supplying digital surveillance equipment, and to persuade ICT companies to ensure they do not contribute to digital authoritarianism. Its moves in relation to Hong Kong provide the most significant, concrete example of this. Considered as a whole, these actions constitute a more multi-pronged approach than was apparent earlier in the 2010s. Still, it is clear that the EU toolbox does not yet fully cover all digital challenges, and that some of the emerging techniques of social control, health-system management, and advanced AI described in previous chapters have not leant themselves easily to EU foreign policy tools, and are only just beginning to be included in EU external dialogues.

**Efficiency:** The EU has made some impacts on a relatively low-cost basis. While it has invested increasing amounts of money in digital initiatives in third countries, funding in this area is still relatively modest. There remains scope for the EU to significantly to ramp up the promising work it has embarked upon through digital funding programmes in recent years. To date, the EU has not been willing to incur significant costs in terms of letting trends in digital repression impact on its commercial and strategic interests. It will need to consider more carefully whether this caution might result in higher 'costs' in the longer term.

**Sanctions and conditionality:** While the EU has fine-tuned its use of restrictive measures related to democracy and human rights, it remains uncertain how relevant these are in response to the digital aspects of repression and rights abuses – as opposed to coups, stolen elections and egregious human rights abuses in violent contexts, where the EU has been more likely to impose sanctions. The EU has become better at monitoring online problems, but it is often difficult to separate these out from other policy concerns in terms of on-the-ground responses.

The EU's new cyber sanctions regime could mark a significant change in this regard. For now, however, this is designed to respond to digital influence operations against the EU, rather than digital forms of authoritarian control within third countries – even if, in practice, there is overlap between these two phenomena. The EU's new Global Human Rights Sanctions regime will target individuals, entities, and bodies. Still, this may not be an instrument relevant to the more structural or institutional levels of states' digital repression, which extend far beyond the actions of a few individuals or entities.

**Resources:** Resources still need to be increased if the EU is to make any significant headway against digital repression. Despite funding increases, funds for democracy and human rights have been limited, relative to other areas of EU spending. The EIDHR has been the smallest of all EU funding instruments, and the EU's other funding instruments have remained rather under-utilised for human rights and democracy in general, and for digital elements of this agenda in particular.

EU external funding has supported an increasing number of digital rights initiatives. Still, there remains considerable scope to increase these allocations to make digital issues a clearer priority element of external democracy and human rights support. There are countries suffering especially severe digital repression in places, where this part of the EU's toolbox has not yet proven relevant. China is a notable omission from digital funding profiles, as any kind of civil society support there has become extremely difficult. While the EU's new 2021–2027 budget includes a modest increase in human rights and democracy funds, it is too early to ascertain the extent to which the new streamlined funding instruments will focus on digital repression. Some interviewees expressed concern that the new multiannual financial framework (MFF) appears to accord greater priority to security and migration issues, raising the perennial question of inter-issue trade-offs.

**Digital distortion in elections:** The EU's tentative moves to build digital considerations into its electoral missions are an important step forward, but will need to be expanded to other countries and benefit from higher resource levels and political backing if it is to have significant impact. It would be valuable to use this change as a base from which the EU can link together its electoral work with long-term capacity

building on digital empowerment within civil society and other instruments. EU policymakers have long recognised the need to make stronger connections between electoral missions and other elements of democracy support; the rise in digital campaigning and online distortion to democratic processes make this an even more urgent imperative.

**Gradual democratic backsliding:** A more general shortcoming comes from the fact that digital repression can often be subtle and accumulate incrementally. The EU tends to clearly react to dramatic interruptions of constitutional processes and obviously manipulated elections, but struggles to respond to these more gradual threats. Many regimes that are not fully authoritarian are assertive users of digital control tactics, yet these are the kind of regimes that the EU has sought to engage for other policy aims, neglecting to foreground the insidious impact of such digital repression.

**Technocratic governance focus:** The EU still also needs to grasp the highly political nature of digitally-driven challenges to democracy and human rights. A lot of European funding has been relatively technical in nature, as it has focused on state institutions. Most EU political aid has aimed for better technical governance standards, economic development, and social service delivery. Around two-thirds of EU development aid for 'good governance' has gone to governments and state institutions[372]. It is doubtful that this is the optimal strategy for dealing with the specific challenges of digital repression. This requires a more political approach to human rights and democracy, which does not rely so heavily on such technocratic cooperation. While the EU has improved its policy tools is recent years, it cannot yet be concluded that it has yet made a complete transition.

**Is digital repression a primary geopolitical interest?** Tensions exist between the EU's digital geopolitics and its commitments to advance democracy and human rights. It has shifted to prioritising digital sovereignty and boosting its relative power in technology against other powers. This is arguably beginning to side-line the rights dimension of digital strategies, and taking the EU back to a highly securitised approach to technological challenges, reminiscent of the early use of the cybersecurity concept. For all of the improvements in EU funding instruments and digital projects in third countries, it is not clear that, at the highest political level, all EU institutions and governments see the surge in digital authoritarianism itself as a geopolitical issue.

# 5 Conclusions and recommendations

The proliferation of new and emerging technologies over the past two decades has significantly expanded states' toolkits for repression and social control, deepening human rights problems. While they still have positive potential to enhance democratic values and human rights, these technologies are now also actively deployed and shaped by many repressive regimes to their own strategic advantage.

Globally and regionally, efforts have been made to tackle the challenge that digital technologies can pose to human rights, but much remains to be done. The EU must both enrich global legal and standard-setting efforts, and also improve its own core foreign policy instruments. The EU's foreign policy toolbox has become more comprehensive in the last several years, as the EU has added a number of different strands to its efforts against digital authoritarianism. The challenge of digitally-led authoritarianism has continued to deepen, however, and the EU will need to look for ways to continue fine-tuning and adding to this toolbox. A core finding that runs through this report is that the EU has undertaken many valuable and well-designed policy initiatives in this field, but still has to decide whether tackling digital repression is a core geopolitical interest at the highest political level.

In order to take the EU's fledgling efforts against digital repression further, a series of recommendations is offered below that encompass both the international human rights framework and the EU's own, more

[372] I. Zamfir, 'Democracy support in EU external policy', European Parliament Research Service Briefing, 2018, p. 7.

specific, foreign policy framework. These two levels are equally important and need to dovetail with each other more effectively if the EU is to advance a fully comprehensive and multi-level approach to digital repression.

**Extending the global reach of EU values through the regulation of new technologies**

- All actors in the EU, including the EP and the human rights community, should push strongly for a comprehensive, binding legal instrument to address the specific challenges posed by AI-driven technologies. This should incorporate human rights safeguards into the entire life cycle of these technologies, including their design, deployment, and implementation, as well as into the full 'datafication cycle'. The EU's efforts to build its own legal framework for the development, design and application of AI technology should not be advanced in isolation from the existing instruments of different human rights organisations or their future improvement, such as the CoE's potentially binding treaty on AI, which is currently under consideration. The European Commission should work towards ensuring consistency between EU and CoE legal frameworks on AI, as the latter could serve as a vehicle to promote the EU's approach within non-EU CoE Member States, and potentially also beyond CoE countries[373], therefore helping to fulfil the Commission's goal to 'bring the Union's approach to the global stage and build a consensus on human-centric AI'[374]. The EP could contribute to global norms in particular by advancing dialogue with the US Congress to try to develop more common understandings, in particular on the norms governing AI and how these impact on human rights questions in both US and EU foreign policies.

- In light of its position as a global standard-setting actor, several other EU developments can help to reinforce multilateral efforts to strengthen the link between human rights and new technologies. This includes, in particular, GDPR, as well as planned or pending legislative initiatives, such as the DSA-DMA package and the EDAP, or possible future instrument(s) concerning mandatory due diligence for companies[375]. Additionally, the 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights'[376] could be used to develop more practical guidance on the application of the UN Guiding Principles to Digital Technologies, while the work of the EU Agency for Fundamental Right (FRA) in AI and discrimination[377] and/or facial recognition[378] could support human rights-based responses to tackling the rise of biometric surveillance in many parts of the world. These initiatives need to be incorporated fully into the EU's ongoing dialogues with human rights organisations as a basis for tightening the human rights legal framework in this area, as well as in direct dialogue with partner countries across the globe. The EU could do more to promote its emerging standards for online platform regulation in third countries, where such rules and regulations remain much weaker.

**Putting more pressure on third countries**

- In addition to all these ideas related to legal instruments, standard-setting, and stakeholder dialogue, the EU needs to include digital repression as a more central part of its high-level diplomacy and geopolitical strategies. Despite the rhetoric around digital repression and authoritarianism spreading globally, in practice, the EU places many other issues higher on its list of priorities with other governments. While seeking better global standard-setting, the EU cooperates on a range of security and commercial issues with some of the most digitally repressive regimes in the world, and has made moves to improve relations

[373] Provided the future CoE instrument, like the 108+ or Budapest Conventions, is open for accession by States that are non-contracting parties of the CoE.
[374] European Commission (2019), 'Building Trust in Human-Centric Artificial Intelligence' Communication.
[375] RBC (2020), European Commission promises mandatory due diligence legislation in 2021.
[376] EU European Commission (2014), ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights.
[377] FRA (2018), #BigData: Discrimination in data-supported decision making.
[378] FRA (2019), Facial recognition technology: fundamental rights considerations in the context of law enforcement.

with such powers. For this to change, the EU must understand such digital trends as a core element of its geopolitical panorama, and not a minor human rights add-on to its core diplomacy.

- In order to make the many multilateral standard-setting forums and exercises more meaningful, the EU should link these to on-the-ground political developments. The EP should play a prominent role in pushing for the EU's range of dialogues on human rights and positions in multilateral forums to address such developments, and not to focus solely on generic internet and digital standards abstracted from national political challenges. Rules, standards, and dialogues need to address concrete crisis situations where digital repression is mobilised at specific moments to deepen authoritarianism. In this, the EU needs to move beyond its much-improved capacities for early warning (including of threats to democracy and human rights) to early action.

- Sanctions are unlikely to be the leading instrument in EU human rights policies, but modest scope may exist to tighten the link between the Union's restrictive measures and digital repression. The 2015 EP resolution mentioned in the previous chapter called for essential elements clauses referring specifically to the need to respect 'digital freedoms', and for unhindered access to the internet, to be included in all new trade agreements. While the EU invokes such clauses relatively infrequently, this would still be a useful step to increase the importance of this issue on the EU's external agenda. The new Global Human Rights Sanctions regime could also be widened by referring more explicitly and extensively to the multiple strands of digital repression covered in this study. The EU still needs to invest in the capacity and monitoring necessary to identify and unpack overt and more subtle forms of digital repression, and stipulate how they contribute to gross human rights violations of the type that might be liable to restrictive measures. This is a difficult task, as regimes' digital tactics are nested within their wider range of power-maintenance strategies, but it might help to check the most draconian cases of digital repression. Even if sanctions need to be used sparingly, some regimes' use of digital control is, at points, so severe that the EU should be willing to consider more concrete responses.

- The EU could and should use positive conditionality more systematically to leverage positive changes away from digital repression. Where third-country governments agree to work with the Union to reform restrictive laws and incorporate international standards, the EU should respond with additional aid, trade, and strategic benefits. This graded approach to political leverage would help deal with the problem of gradual autocratisation that the previous chapter outlines as one of the EU's Achilles heels in recent years.

- Approaches to digital technology need to move away from security- , and towards rights-based measures. The EU's fast-growing array of cyber-security work has begun to incorporate a focus on digital rights, but a lot could (and still needs to) be done to fuse the security and human rights elements of the Union's digital strategies. The same applies to Stratcom, the valuable work of which remains, as yet, somewhat disconnected from core EU human rights and democracy support. The EU would benefit from a formal liaison or contact point to link together the multiple cyber-security and human rights initiatives described above. EU pressure on cyber-security should align with pressure on human rights and democracy concerns.

**Putting more pressure on the private sector**

- The EU should increase the pressure it puts on private company operations in third countries, extending the ways it has begun to push them to adhere to more rigorous standards within the EU itself in recent years. This could take the form of a code or set of guidelines pertinent to companies' stances on internet shutdowns and acute forms of digital repression outside of Europe. Where companies are found to be complicit in such digital repression, guilty of censorship themselves, or in breach of the UN Guiding Principles on Business and Human Rights, the EU might (as suggested in the 2015 EP resolution) subject them to certain forms of penalty, like exclusion from EU contracts – even if, generally, the EU (rightly) continues to prioritise efforts aimed at positive dialogue and cooperation.

- The EU needs to be also more attentive to the problem of 'privatised censorship' – that is, online platforms taking voluntary decisions that have negative effects on freedom of expression, as was recently the case when activists from the MENA region were blocked by Facebook and Twitter (see Chapter 3). As the EU is currently working on a legislative proposal to curb the arbitrariness of such practices of online platforms as part of the DSA-DMA package, it also needs to stress this problem in its external actions. Users in other parts of the world still lack protection against big tech's decisions that undermine their fundamental rights. Given the European Commission's experience in engaging in dialogue with dominant online platforms in the area of content moderation[379], it should extend these efforts to support platforms' user rights in other regions, leading the push for protection against unfair, non-transparent, and arbitrary removals.

**Increasing resources, funding, and capacity**

- The most impressive area of improvement in EU external initiatives is the Union's range of funding for digital rights in third counties. This is important because it seeks to deal with digital repression through the positive approach of equipping local societies to defend their own human rights and explore the positive democratic potential of digital technology. Still, given the relatively modest amount of funding that has so far gone to such digital empowerment projects, the EU could and should significantly increase it. The EU could pick up a suggestion made in the EP's 2015 resolution for a 'human rights and technology fund' to be created under the EIDHR (or now, its thematic successor). The EU has undertaken extremely valuable and creative work in protecting human rights defenders, including through digital tools. The challenge in building from this role will be for the Union to help create longer-term, systemic civic capacities to keep democratic spaces open, through a combination of joint online and offline techniques.

- The EP can play a valuable role here, using its cooperation with parliaments around the world to engage politicians with such civic initiatives as a means of amplifying their political impact. Given its key role in election observation, the EP would also be well placed to support a large-scale expansion of the EU's fledgling and highly welcome efforts to build digital elements into its Election Observation Missions (EOMs) – this would be a natural area of partnership between the EP and the European External Action Service (EEAS). The EP could also push for increased levels of support to the European Endowment for Democracy (EED) and other foundations that are well equipped to take risks in pushing back against digital repression in the most difficult contexts.

- The EU should invest more resources in fostering wider coalitions of engagement. Any work in the field of human rights and new technologies, whether undertaken by human rights organisations or the EU, in an internal or external context, requires multi-stakeholder engagement. Apart from enhanced cooperation with the corporate sector, it is also essential to include other actors, particularly civil society and academia. Furthermore, such work requires adequate resources (human resources, in particular) to close the 'knowledge gap' between legal/human rights and technology experts.

- The EU should provide more resources to strengthen the rights-oriented monitoring of surveillance equipment exports, specifically. While the recast of the EU Dual-Use Regulation represents an important – if belated – step forward, tighter vigilance will be needed over the global spread of surveillance equipment beyond the tightly drawn terms of this regulation. The EP should support a dedicated initiative to monitor surveillance equipment exports from the EU, and – far from decreasing its focus on this issue now that the regulation is agreed – commit to working alongside civil society organisations to raise the profile of this issue.

[379] See: EU Code of Practice on disinformation and Code of Conduct on countering illegal hate speech online.

In summary, there is scope for the EU to take the multiple levels at which it has begun to design responses to digital repression around the world even further. The EP is well placed to play a prominent role in assisting with and critically monitoring this area of policy development. One cross-cutting challenge is to ensure that the various strands of policy join together in a more coherent and high-profile commitment to tempering digital repression. This trend is now of such a serious magnitude that it cannot be tackled through sporadic funding projects or multilateral standard-setting dialogues only; an EU policy that is fully commensurate with the scale of the technological challenge would place this issue at the highest political level of its overarching foreign policy priorities. For all the progress the EU has made in recent years, this necessary step is still to be taken.

# Annex 1: Sources of information

## Bibliography

### Primary sources

African Commission on Human and Peoples' Rights, 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa', 2019. Available at: www.achpr.org/pressrelease/detail?id=8

African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (revised), 2019. Available at: https://www.achpr.org/legalinstruments/detail?id=69

African Special Rapporteur on Freedom of Expression and Access to Information, 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the situation of freedom of expression and access to information in the Republic of Zimbabwe', 2019. Available at: www.achpr.org/pressrelease/detail?id=9

African Union, 'Chart of signatures and ratifications of the African Charter on Human and Peoples' Rights ('AChHPR')'. Available at: https://www.achpr.org/statepartiestotheafricancharter#:~:text=The%20African%20Charter%20on%20Human,Charter%20on%2023%20October%202013

Community Court of Justice of the Economic Community of West African States (ECOWAS), 'Amnesty International & Others v. The Togolese Republic', ECW/CCJ/JUD/09/20, 25 June 2020. Available at: http://prod.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_09_20.pdf

Council of Europe Ad Hoc Committee on Artificial Intelligence (CoE CAHAI), 'Feasibility study', 2020. Available at: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

Council of Europe Commissioner for Human Rights, 'Issue Paper on Democratic and Effective Oversight of National and Security Services', 4 May 2015. Available at: https://www.dcaf.ch/council-europe-commissioner-human-rights-issue-paper-democratic-and-effective-oversight-national

Council of Europe Commissioner for Human Rights, 'Positions on Counter-Terrorism and Human Rights Protection', 5 June 2015. Available at: https://rm.coe.int/16806db6b2

Council of Europe Commissioner for Human Rights, 'Press freedom must not be undermined by measures to counter disinformation about COVID-19', 2020. Available at: www.coe.int/en/web/commissioner/thematic-work/covid-19/-/asset_publisher/5cdZW0AJBMLl/content/press-freedom-must-not-be-undermined-by-measures-to-counter-disinformation-about-covid-19

Council of Europe Commissioner for Human Rights, 'Speech at the conference Human Rights in the Era of AI Europe as international Standard Setter for Artificial Intelligence', 20 January 2021. Available at: https://rm.coe.int/german-cm-presidency-high-level-conference-human-rights-in-the-era-of-/1680a12379

Council of Europe Commissioner for Human Rights, 'Speech at the Human Rights talk: Covid-19 and Human Rights – Lessons learned from the pandemic', 10 December 2020. Available at: https://search.coe.int/commissioner/Pages/result_details.aspx?ObjectId=0900001680a0a7c3

Council of Europe Commissioner for Human Rights, 'Unboxing artificial intelligence: 10 steps to protect human rights', 2019. Available at: https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights

Council of Europe Committee of Ministers, 'Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes', 2019. Available at: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

Council of Europe Committee of Ministers, 'Recommendation CM/Rec (2019)2 on the protection of health-related data',2019. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e

Council of Europe Committee of Ministers, 'Recommendation of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors', CM/Rec(2016)4, 2016. Available at: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2016-4-of-the-committee-of-ministers-to-member-states-on-the-protection-of-journalism-and-safety-of-journalists-and-other-media-

Council of Europe Committee of Ministers, 'Recommendation on preventing and combating sexism', CM/Rec(2019)1, 2019. Available at: https://rm.coe.int/168093b26a

Council of Europe Committee of Ministers, 'Recommendation on the human rights impacts of algorithmic systems', CM/Rec(2020)1, 2020. Available at: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016809e1154

Council of Europe Committee of Ministers, 'Recommendation on the roles and responsibilities of internet intermediaries', CM/Rec(2018)2, 2018. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14

Council of Europe Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing (CoE T-PD), 'Guidelines on Artificial Intelligence and Data Protection', T-PD(2019)01, 25 January 2019. Available at: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

Council of Europe Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing (CoE T-PD), 'Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data', 2017. Available at: https://rm.coe.int/16806ebe7a

Council of Europe Cybercrime Convention Committee (T-CY), 'Mapping study on cyberviolence', 2018. Available at: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

Council of Europe European Committee on Crime Problems (CPDC), 'Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law', 2020. Available at: https://rm.coe.int/cdpc-2020-3-feasibility-study-of-a-future-instrument-on-ai-and-crimina/16809f9b60

Council of Europe Secretary General 'Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis: A toolkit for member states available in different languages', 2020. Available at: https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40

Council of Europe, 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems', ETS No.189, 2003. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Council of Europe, 'Artificial Intelligence – Intelligent Politics Challenges and opportunities for media and democracy', Background Paper, 2020. Available at: https://rm.coe.int/cyprus-2020-ai-and-freedom-of-expression/168097fa82

Council of Europe, 'Chart of signatures and ratifications of the European Convention of Human Rights ('ECHR')'. Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures

Council of Europe, 'Chart of signatures and ratifications of the European Social Charter ('ESC')'. Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/163/signatures

Council of Europe, 'Chart of signatures and ratifications of the Convention 108+'. Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', ETS No. 108., 1981. Available at: https://rm.coe.int/1680078b37

Council of Europe, 'Convention on Cybercrime', ETS No.185, 2001. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

Council of Europe, 'Convention on preventing and combating violence against women and domestic violence', CETSNo.210, 2011. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008482e

Council of Europe, 'Digital solutions to fight COVID-19. 2020 Data Protection Report', 2020. Available at: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c

Council of Europe, 'European Convention on Human Rights ('ECHR')', 4 November 1950. Available at: https://www.echr.coe.int/documents/convention_eng.pdf

Council of Europe, 'Chart of signatures and ratifications of the Convention on Cybercrime'. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Council of Europe, European Committee on Crime Problems (CDPC), 'Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law', 4 September 2020. Available at: https://rm.coe.int/cdpc-2020-3-feasibility-study-of-a-future-instrument-on-ai-and-crimina/16809f9b60

Council of Europe, The Chair of the Committee of Convention 108, the Data Protection Commissioner of the Council of Europe, 'Joint Statement on the right to data protection in the context of the COVID-19 pandemic', 30 March 2020. Available at: https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter

Council of Europe, The Chair of the Committee of Convention 108, the Data Protection Commissioner of the Council of Europe, 'Joint Statement on Digital Contact Tracing', 28 April 2020. Available at: https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7

Council of the European Union, 'Council conclusions on Human Rights and Democratisation in third countries', 2985th Foreign Affairs Council meeting, Brussels, 8 December 2009. Available at: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/111819.pdf

Council of the European Union, 'Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States', 7299/19, 14 May 2019. Available at: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

Council of the European Union, 'COVID-19: Council adopts conclusions on human rights-based recovery', 22 February 2021. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/02/22/covid-19-council-adopts-conclusions-on-human-rights-based-recovery/

Council of the European Union, 'EU Human Rights Guidelines on Freedom of Expression Online and Offline', Foreign Affairs Council, 12 May 2014. Available at: www.consilium.europa.eu/media/28348/142549.pdf

Council of the European Union, 'EU Strategic Framework and Action Plan on Human Rights and Democracy', 11855/12, 25 June 2012. Available at: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf

Council of the European Union, 'Council Conclusions on Democracy', 12836/19, 14 October 2019. Available at: https://data.consilium.europa.eu/doc/document/ST-12836-2019-INIT/en/pdf

Democracy Support and Election Coordination Group. Available at: https://www.europarl.europa.eu/globaldemocracysupport/en/home/democracy-group

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and The Council. Human Rights and Democracy at the Heart of EU external actions- Towards More Effective Approach', 12 December 2011. Available at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0886:FIN:EN:PDF

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'Cybersecurity strategy of the European Union: an open, safe and secure cyberspace', JOIN(2013) 1, 7 February 2013. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission and High Representative of The Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions. Review of the European Neighbourhood Policy', JOIN(2015), 18 November 2015. Available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/joint-communication_review-of-the-enp.pdf

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Staff Working Document. Report on EU Enhanced Engagement with three Everything But Arms beneficiary countries: Bangladesh, Cambodia and Myanmar', SWD(2020) 19, 10 February 2020. Available at: https://ec.europa.eu/transparency/regdoc/rep/10102/2020/EN/SWD-2020-19-F1-EN-MAIN-PART-1.PDF

European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, 'EU Action Plan on Human Rights and Democracy 2020-2024', JOIN (2020)5, 23 March 2020. Available at: https://ec.europa.eu/transparency/regdoc/rep/10101/2020/EN/JOIN-2020-5-F1-EN-MAIN-PART-1.PDF

European Commission Directorate-General for Communications Networks, Content and Technology, 'No Disconnect Strategy Workshop: European Capability for Situational Awareness', (ECSA), 2012. Available at: https://ec.europa.eu/digital-single-market/en/news/no-disconnect-strategy-workshop-european-capability-situational

European Commission for the Efficiency of Justice of the Council of Europe (CoE CEPEJ), 'European Ethical Charter for the use of artificial intelligence in judicial systems and their environment', 2018. Available at: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment

European Commission, 'Building Trust in Human-Centric Artificial Intelligence', Communication, 2019. Available at: https://ec.europa.eu/jrc/communities/en/community/digitranscope/document/building-trust-human-centric-artificial-intelligence

European Commission, 'European consensus on development', 2017. Available at: https://ec.europa.eu/international-partnerships/european-consensus-development_en

European Commission, 'European Democracy Action Plan', 2020. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2250

European Commission, 'Increasing the Impact of EU Development Policy: An Agenda for Change', COM(2011) 637, 2011. Available at: https://knowledge4policy.ec.europa.eu/publication/agenda-change-com2011-637-final_en

European Commission, 'Press release: Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally', 12 December 2011. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_11_1525.

European Commission, 'Regulation on data governance - Questions and Answers', 2020. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2103

European Commission, 'The List of all EU sanctions'. Available at: www.sanctionsmap.eu/#/main

European Court for Human Rights, 'Vladimir Kharitonov v. Russia', 10795/14, 23 June 2020. Available at: http://hudoc.echr.coe.int/eng?i=001-203177

European Court of Auditors, 'Challenges to effective EU cybersecurity policy', Briefing paper, 2019. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

European Court of Human Rights, 'Bulgakov v. Russia', 20159/15. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-203181%22]}

European Court of Human Rights, 'Engels v. Russia', 61919/16, 23 June 2020. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-203180%22]}

European Court of Human Rights, 'Fact sheet on Mass surveillance case law', 2020. Available at: www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf

European Court of Human Rights, 'Kablis v. Russia', 59663/17, 30 April 2019. Available at: https://laweuro.com/?p=2802

European Court of Human Rights, 'OOO Flavus and Others v. Russia', 12468/15, 23 June 2020. Available at: https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-203178%22]}

European Court of Human Rights, 'Zakharov v. Russia', No. 47143/06, 4 December 2015. Available at: https://fra.europa.eu/en/caselaw-reference/ecthr-application-no-4714306-judgment

European External Action Service (EEAS), 'A stronger Europe: a global strategy for the European Union's foreign and security policy', 2017. Available at: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

European Parliament Democracy Support and Election Coordination Group, 'Annual Work Programme 2020', 2020. Available at: https://www.europarl.europa.eu/cmsdata/212226/DEG_Annual_Work_programme_2020-links_index.pdf

European Parliament, 'Resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy', 2012/2094(INI), 11 December 2012. Available at: www.europarl.europa.eu/doceo/document/TA-7-2012-0470_EN.html

European Parliament, 'Resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries', 2014/2232(INI), 2015. Available at: www.europarl.europa.eu/doceo/document/TA-8-2015-0288_EN.html

European Parliamentary Research Service, 'Review of dual-use export controls', January 2021. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI%282016%29589832_EN.pdf

European Union Agency for Fundamental Rights (FRA), '#BigData: Discrimination in data-supported decision making', 2018. Available at: https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making

European Union Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 2019. Available at: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

General Secretariat of the Council of the European Union, 'Council conclusions on internet governance', 16200/14, 27 November 2014. Available at: http://italia2014.eu/media/3769/council-conclusions-on-internet-governance.pdf

GNI, 'Global Network Initiative Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 2015

IACHR Special Rapporteur for Freedom of Expression, UN Special Rapporteur on freedom of expression and OSCE Representative on Freedom of the Media, 'COVID-19: Governments must promote and protect access to and free flow of information during pandemic – International experts', Press release 58/20, 2020. Available at: www.oas.org/en/iachr/expression/showarticle.asp?artID=1170&lID=1

ICFJ-UNESCO, 'Global Study: Online Violence Against Women Journalists. A Global Snapshot of Incidence and Impacts', 2020. Available at: www.icfj.org/sites/default/files/2020-12/UNESCO%20Online%20Violence%20Against%20Women%20Journalists%20-%20A%20Global%20Snapshot%20Dec9pm.pdf

Indian Ministry of Electronics and Information Technology, 'The Information Technology [Intermediaries Guidelines (Amendment) Rules', 24 December 2018. Available at: meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

Inter-American Commission on Human Rights and IACHR Special Rapporteur for Freedom of Expression, 'States of the Region must Accelerate Universal Internet Access Policies during the COVID-19 Pandemic and Adopt Differentiated Measures to Incorporate Groups in Vulnerable Situations', 2020. Available at: https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1182&lID=1

Inter-American Commission on Human Rights, 'Pandemic and human rights in the Americas', Resolution no. 1/2020, 2020. Available at: www.oas.org/en/iachr/decisions/pdf/Resolution-1-20-en.pdf

OHCHR Accountability and Remedy Project. Available at: www.ohchr.org/EN/Issues/Business/Pages/OHCHRaccountabilityandremedyproject.aspx

Organisation of American States, 'Chart of signatures and ratifications of the American Convention on Human Rights ('ACHR')'. Available at: http://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights_sign.htm

Organisation of American States, 'Chart of signatures and ratifications of the Additional Protocol to The American Convention on Human Rights in the Area of Economic, Social and Cultural Rights 'Protocol of San Salvador''. Available at: http://www.oas.org/juridico/english/sigs/a-52.html

Organisation of American States, Office of the Special Rapporteur for Freedom of Expression and Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet', 2013. Available at: www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf

Organisation of American States, Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere', Press Release R80/15, 2015. Available at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=998&lID=1

OSCE Representative on Freedom of the media, 'Impact of Artificial Intelligence'. Available at: https://www.osce.org/fom/ai-free-speech

OSCE, 'Communiqué by the OSCE RFoM on Media Pluralism, Safety of Female Journalists and Safeguarding Marginalized Voices Online', 2019. Available at: www.osce.org/representative-on-freedom-of-media/411917

OSCE, 'Joint declarations. Available at https://www.osce.org/fom/66176

OSCE, 'Recommendations on Countering Online Abuse of Female Journalists', 21 October 2015. Available at: www.osce.org/fom/193556

OSCE, 'Safety of Female Journalists', Resource guide, 2020, Available at:www.osce.org/files/f/documents/2/9/468861_0.pdf

Parliamentary Assembly of the Council of Europe (PACE), 'Resolution on Mass Surveillance 2045', 2015. Available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692

Parliamentary Assembly of the Council of Europe (PACE), 'Technological convergence, artificial intelligence and human rights', Recommendation 2102 (2017), 2017. Available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

The Law Library of Congress, 'Freedom of Expression during COVID-19', 2020. Available at: http://www.loc.gov/law/help/covid-19-freedom-of-expression/freedom-of-expression-during-covid-19.pdf

The Office of the High Commissioner for Human Rights (UN Human Rights), 'State duty to protect human rights' in: 'The Guiding Principles on Business and Human Rights. Implementing the United Nations 'Protect, Respect and Remedy' Framework', 2011. Available at: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

The Wassenaar Arrangement Secretariat. Available at: www.wassenaar.org

UN and World Health Organisation, 'Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing', 2020. Available at: www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

UN Committee on the Elimination of Racial Discrimination, 'Preventing and Combating Racial Profiling by Law Enforcement Officials', General recommendation No. 36, 2020. Available at: https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/1_Global/CERD_C_GC_36_9291_E.pdf

UN Conference on Trade and Development (UNCTD), 'Digital Economy Report 2019', 2019. Available at: https://unctad.org/system/files/official-document/der2019_en.pdf

UN Data Revolution, 'A World that Counts Mobilising the Data Revolution for Sustainable Development', 2014. Available at: www.undatarevolution.org/report/

UN General Assembly, 'Resolution on the right to privacy in the digital age', A/RES/71/199, 2017. Available at: https://undocs.org/en/A/RES/71/199

UN General Assembly, 'Resolution on the safety of journalists and the issue of impunity', A/RES/72/175, 2017. Available at: https://digitallibrary.un.org/record/1467885

UN General Assembly, 'Right to Privacy in the Digital Age', Resolution A/RES/73/179, 2018. Available at: https://digitallibrary.un.org/record/1661346

UN General Assembly, 'The Right to Privacy in the Digital Age', Resolution 68/167, A/RES/68/167, 2013. Available at: www.ohchr.org/EN/Issues/DigitalAge/Pages/InternationalStandardsDigitalPrivacy.aspx

UN General Assembly, 'The Right to Privacy in the Digital Age', Resolution 28/16, A/HRC/RES/28/16, 2015. Available at: www.ohchr.org/EN/Issues/DigitalAge/Pages/InternationalStandardsDigitalPrivacy.aspx

UN General Assembly, Resolution A/RES/75/176, 2020. Available at: https://undocs.org/A/RES/75/176

UN High Commissioner for Human Rights, 'Report A/HRC/27/37', 2014. Available at: www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalReports.aspx

UN High Commissioner for Human Rights, 'Report on the right to privacy in the digital age', A/HRC/39/29, 2018. Available at: www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalReports.aspx

UN High Commissioner for Human Rights, 'UN experts call for investigation into allegations that Saudi Crown Prince involved in hacking of Jeff Bezos' phone', 22 January 2020. Available at: www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488&LangID=E

UN HLPDC, 'The Age of Digital Independence', 2019. Available at: www.un.org/en/digital-cooperation-panel/

UN Human Right Council, 'Resolution 32/10', 15 July 2016. Available at: https://undocs.org/A/HRC/RES/32/10

UN Human Right Council, 'Resolution 38/13', 18 July 2018. Available at: https://undocs.org/A/HRC/RES/38/13

UN Human Right Council, 'Resolution 44/15', 23 July 2020. Available at: https://undocs.org/A/HRC/RES/44/15

UN Human Rights Committee, 'Concluding Observations on the Sixth Periodic Report of Italy', Doc. CCPR/C/ITA/CO/6, 2017. Available at: https://www.refworld.org/docid/591e9a6b4.html

UN Human Rights Committee, 'General comment no. 37 on the right of peaceful assembly', 2020. Available at: https://digitallibrary.un.org/record/3884725

UN Human Rights Council 'Resolution on the promotion and protection of human rights in the context of peaceful protests', A/HRC/44/L.11, 2020. Available at: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/44/L.11

UN Human Rights Council, 'New and emerging digital technologies and human rights, Resolution no. A/HRC/RES/41/11', 2019. Available at: https://undocs.org/A/HRC/RES/41/11

UN Human Rights Council, 'New and emerging digital technologies and human rights'. Available at: https://www.ohchr.org/EN/HRBodies/HRC/AdvisoryCommittee/Pages/DigitalTechnologiesandHR.aspx

UN Human Rights Council, 'Report of the independent international fact-finding mission on Myanmar', A/HRC/39/64, 2018. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.docx

UN Human Rights Council, 'Resolution 17/4', 2011. Available at: https://undocs.org/en/A/HRC/RES/17/4

UN Human Rights Council, 'Resolution 26/22', 23 July 2020. Available at: https://undocs.org/A/HRC/RES/44/15

UN Human Rights Council, 'Resolution 26/9. Elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights', 14 July 2014. Available at: https://undocs.org/A/HRC/RES/26/9

UN Human Rights Council, 'Resolution 39/6', 27 September 2018. Available at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session39/Pages/ResDecStat.aspx

UN Human Rights Council, 'Resolution A/HRC/32/L.20', 2016

UN Human Rights Council, 'Resolution A/HRC/44/L.11', 2020

UN Human Rights Council, 'Resolution on 'the promotion, protection, and enjoyment of human rights on the Internet'', A/HRC/20/L.13, 2012. Available at: https://undocs.org/A/HRC/20/L.13

UN Human Rights Council, 'Resolution on accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts', A/HRC/38/L.6, 2018. Available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/195/60/PDF/G1819560.pdf?OpenElement

UN Human Rights Council, 'Resolution on Freedom of Opinion and Expression', A/HRC/44/12, 2020. Available at: https://undocs.org/en/A/HRC/44/L.18/Rev.1

UN Human Rights Council, 'Resolution on the promotion, protection and enjoyment of human rights on the Internet', A/HRC/32/L.20, 27 June 2016. Available at: https://undocs.org/A/HRC/32/L.20

UN Human Rights Council, 'Resolution on the safety of journalists, A/HRC/RES/39/6', 2018. Available at: https://www.right-docs.org/doc/a-hrc-res-39-6/

UN Human Rights Council, 'The Right to Privacy in the Digital Age', Resolution A/HRC/34/L,7, 2017. Available at: https://undocs.org/A/HRC/34/L.7/Rev.1

UN Human Rights Council, 'New and emerging digital technologies and human rights', Resolution no. A/HRC/RES/41/11, 2019. Available at https://undocs.org/A/HRC/RES/41/11

UN Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/HRC/38/35', 2018. Available at: www.undocs.org/A/HRC/38/35

UN Secretary General, 'Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights', A/HRC/43/29, 2020. Available at: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf

UN Secretary General, 'Roadmap for Digital Cooperation', 2020. Available at: www.un.org/en/content/digital-cooperation-roadmap

UN Secretary General, 'Strategy on new technologies', 2018. Available at: www.un.org/en/newtechnologies

UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 'Racial discrimination and emerging digital technologies: a human rights analysis', A/HRC/44/57, 18 June 2020. Available at: https://undocs.org/en/A/HRC/44/57

UN Special Rapporteur on extreme poverty and human rights, 'Report A/74/493', 11 October 2019. Available at: https://undocs.org/A/74/493

UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Challenges to Freedom of Expression in the Next Decade', 2019. Available at: www.osce.org/representative-on-freedom-of-media/425282

UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and Responses to Conflict Situations', 4 May 2015. Available at: https://www.osce.org/fom/154846

UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Report No. A/HRC/34/61', 2017. Available at: https://www.ohchr.org/documents/issues/terrorism/a-hrc-34-61.pdf

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/70/361', 2015. Available at: https://digitallibrary.un.org/record/805706

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/HRC/23/40', 2013. Available at: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/HRC/29/32', 2015. Available at: https://undocs.org/en/A/HRC/29/32

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/HRC/35/22', 2017. Available at: https://undocs.org/en/A/HRC/35/22

UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 'Raport no. A/HRC/32/38', 2016. Available at: https://undocs.org/en/A/HRC/32/38

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Encryption and anonymity follow-up report', 2018: Available at: www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report no. A/73/348', 2018. Available at: https://undocs.org/pdf?symbol=en/A/73/348

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Surveillance and human rights. Report no. A/HRC/41/35', 2019. Available at: https://undocs.org/A/HRC/41/35

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Report: Disease pandemics and the freedom of opinion and expression', A/HRC/44/49, 2020. Available at: https://undocs.org/en/A/HRC/44/49

UN Special Rapporteur on the right to privacy, 'Report no. A/74/277', 2019. Available at: https://undocs.org/A/74/277

UN Special Rapporteur on the right to privacy, 'Report no. A/75/147', 2020. Available at: https://undocs.org/A/75/147)

UN Special Rapporteur on the right to privacy, 'Report no. A/HRC/37/62', 2018. Available at: https://undocs.org/A/HRC/37/62

UN Special Rapporteur on the Right to Privacy, 'Report no. A/HRC/31/64', 2016. Available at: https://undocs.org/en/A/HRC/31/64

UN Special Rapporteur on the right to privacy, 'Report no. A/HRC/34/60', 2017. Available at: https://undocs.org/A/HRC/34/60

UN Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, 'Report no. A/HRC/38/47', 2018. Available at: https://digitallibrary.un.org/record/1641160

UN Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, 'Report. No. A/HRC/8/5', 2008. Available at: https://digitallibrary.un.org/record/626739

UN, 'Chart of signatures and ratifications of the 4. International Covenant on Civil and Political Rights('ICCPR')'. Available at: https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND

UN, 'Chart of signatures and ratifications of the International Covenant on Economic, Social and Cultural Rights ('ICESCR')'. Available at: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-3&chapter=4&clang=_en

UN, 'Joint statement on data protection and privacy in the COVID-19 response published by various UN agencies: IOM, ITU, OCHA, OHCHR, UNDP, UNEP, UNESCO, UNFPA, UNHCR, UNICEF, UNOPS, UPU, UN Volunteers, UN Women, WFP and WHO', 2020. Available at: www.un.org/sites/un2.un.org/files/joint_statement_on_data_protection_and_privacy_in_covid-19_response.pdf

UN, 'Secretary-General's High-level Panel on Digital Cooperation', 2020. Available at: http://www.un.org/en/digital-cooperation-panel

UN, 'The Impact of digital technologies. Available at: www.un.org/en/un75/impact-digital-technologies

United Nations General Assembly, 'International Covenant on Civil and Political Rights', Resolution 2200A (XXI), 16 December 1966. Available at: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_2200A(XXI)_civil.pdf

United Nations Hub for Human Rights and Digital Technology. Available at: https://www.digitalhub.ohchr.org/

## Secondary sources - books and articles

Adamson, F.B. and Gerasimos, T., 'At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression', Freedom House, 2020. Available at: https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression

AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines', 2019. Available at: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Al-Jizawi, N., Anstis, S., Chan, S., Senft, A. and Deibert, R. J., 'Annotated Bibliography. Annotated. Transnational Digital Repression', Citizen Lab, University of Toronto, 2020. Available at: https://citizenlab.ca/wp-content/uploads/2020/11/Annotated-Bibliography-Transnational-Digital-Threats.pdf

Allen-Ebrahimian, B., 'Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm', International Consortium of Investigative Journalists, 24 November 2019. Available at: https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/

Bavas, J., 'Facial recognition system rollout was too rushed, Queensland police report reveals', ABC, 5 May 2019. Available at: www.abc.net.au/news/2019-05-06/australias-biggest-facial-recognition-roll-out-rushed/11077350

Bressanelli, E., Di Palma, A., Marini, S. and Repetto, E., 'Institutions and foreign interferences', 2020. Available at: www.europarl.europa.eu/RegData/etudes/STUD/2020/655290/IPOL_STU(2020)655290_EN.pdf

Brzozowski, A., 'Commission floats sanctions regime for disinformation offenders', Euractive, 3 December 2020. Available at: http://www.euractiv.com/section/digital/news/commission-floats-sanctions-regime-for-disinformation-offenders/

Bukovska, B., 'Spotlight on Artificial Intelligence and Freedom of Expression #SAIFE', OSCE, 2020. Available at: https://www.osce.org/files/f/documents/9/f/456319_0.pdf

Burrows, M. and Mueller-Kaler J., 'Smart Partnerships amid Great Power Competition: AI, China, and the Global Quest for Digital Sovereignty', Atlantic Council, 2021. Available at: http://www.atlanticcouncil.org/wp-content/uploads/2021/01/Smart-Partnerships-2021-Report-1.pdf

Christou, G., 'Cybersecurity in the European Union: resilience and adaptability in governance', London, Palgrave, 2015.

Claessen, E., 'Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU', Journal of Cyber Policy, 5 (1), 2020. Available at: www.tandfonline.com/doi/full/10.1080/23738871.2020.1728356

Csernatoni, R., 'New states of emergency: normalizing technosurveillance in the time of COVID-19', Global Affairs, 6, 2020. Available at: https://www.tandfonline.com/doi/abs/10.1080/23340460.2020.1825108

Dalmasso, E., Del Sordi, A., Glasius, M., Hirt, N., Michaelsen, M., Mohammad, A. S., and Moss, D., 'Intervention: Extraterritorial Authoritarian Power', Political Geography, 2017. Available at: https://doi.org/10.1016/j.polgeo.2017.07.003

Danaher, J., et al., 'Algorithmic governance: Developing a research agenda through the power of collective intelligence', Big Data & Society, 4 (2), 2017. Available at: https://journals.sagepub.com/doi/full/10.1177/2053951717726554

De Gregorio, G. and Stremlau, N. 'Internet Shutdowns and the Limits of Law', International Journal of Communication, 14, 2020. Available at: https://ijoc.org/index.php/ijoc/article/download/13752/3183

Deibert, R. 'Authoritarianism Goes Global: Cyberspace Under Siege', Journal of Democracy, 26 (3), 2015. Available at: https://www.journalofdemocracy.org/articles/authoritarianism-goes-global-cyberspace-under-siege/

Dragu, T. and Lupu, Y., 'Digital Authoritarianism and the Future of Human Rights', International Organisation, October 2020. Available at: https://doi.org/10.1017/S0020818320000624

Erixon, F. and Lee-Makiyama, H., 'Digital authoritarianism: Human rights, geopolitics and commerce', No. 5/2011, ECIPE Occasional Paper, 2011. Available at: www.econstor.eu/handle/10419/174715

Eskandar, W., 'How Twitter is gagging Arabic users and acting as morality police', Open Democracy, 23 October 2019. Available at: www.opendemocracy.net/en/north-africa-west-asia/how-twitter-gagging-arabic-users-and-acting-morality-police

Faracik, B., 'Implementation of the UN Guiding Principles on Business and Human Rights', 2017. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/578031/EXPO_STU(2017)578031_EN.pdf.

Feldstein, S., 'The Global Expansion of AI Surveillance', Carnegie Endowment for International Peace, 2019. Available at: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Feldstein, S., 'When it comes to digital authoritarianism, China is a challenge- but not only', War on Rocks, 2020. https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/

Garbe, L., 'What we do (not) know about Internet shutdowns in Africa', 29 September 2020. Available at: http://democracyinafrica.org/internet_shutdowns_in_africa

Garside, S., 'Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom', Diss. College of Europe, 2020. Available at: https://kennisopenbaarbestuur.nl/media/257122/edp_1-2020_garside.pdf

Gebrekidan, S., 'For autocrats and others, coronavirus is a chance to grab even more power', New York Times, 30 March 2020. Available at: https://www.nytimes.com/2020/03/30/world/europe/coronavirus-governments-power.html

Geissbauer, R., Vedso, J. and Schrauf, S., 'Industry 4.0: Building the Digital Enterprise', PwC, London, 2016. Available at: www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

Gifford, C., 'What a sovereign internet could mean for free speech', The New Economy, 6 August 2019. Available at: www.theneweconomy.com/technology/what-a-sovereign-internet-could-mean-for-free-speech

Giles, C., Mwai, P., 'Africa internet: Where and how are governments blocking it?', BBC, 2 November 2020. Available at: www.bbc.com/news/world-africa-47734843

Godfrey, K. and Youngs, R., 'Towards a New EU Democracy Strategy', Carnegie Europe, 2019.

Godfrey, Ken and Youngs, Richard, 'Toward a New EU Democracy Strategy', Working Paper, Carnegie Endowment for International Peace, September 2019.

Gomez, F., Muguruza, C. and Wouters, J., (eds), 'EU human rights and democratisation policies: achievements and challenges', Routledge, London, 2018.

Gorwa, R., Binns, R. and Katzenbach, Ch., 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance', Big Data & Society, 7(1), 2020. Available at: https://policyreview.info/concepts/algorithmic-governance

Gressel, G., 'Protecting Europe against hybrid threats', London, European Council on Foreign Relations, 2020. Available at: https://ecfr.eu/publication/protecting_europe_against_hybrid_threats/

Gritsenko, D. and Wood, M., 'Algorithmic governance: A modes of governance approach', Regulation & Governance, 2020. Available at: https://onlinelibrary.wiley.com/action/showCitFormats?doi=10.1111%2Frego.12367

Hakmeh, J., Peters, A. , 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet', Council on Foreign Relations, 13 January 2020

Harwell, D. and Nakashima, E., 'Federal prosecutors accuse Zoom executive of working with Chinese government to surveil users and suppress video calls', Washington Post, 19 December 2020. Available at: www.washingtonpost.com/technology/2020/12/18/zoom-helped-china-surveillance

Hoffman, S., 'Managing the State: Social Credit, Surveillance and the CCP's Plan for China', in: Wright, N., 'AI, China, Russia, and the Global Order. Technological, Political, Global, and Creative Perspectives', NSI, 2019. Available at: https://nsiteam.com/ai-china-russia-and-the-global-order-technological-political-global-and-creative-perspectives

Kalniete, S., 'Working document on the state of foreign interference in the European Union, including disinformation', Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, 17 December 2020. Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/INGE/DT/2021/01-11/1220809EN.pdf

Kitchin, R., 'Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19', Space and Polity Journal, June 2020. Available at: www.tandfonline.com/doi/full/10.1080/13562576.2020.1770587

Kitchin, Rob, 'Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19', Space and Polity Journal, June 2020

Kleemola, K., Crete-Nishihata, M. and Scott-Railton, J., 'Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114', Citizen Lab, University of Toronto, 15 June 2015. Available at: https://citizenlab.ca/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114

Knockel, J., Parsons, C., Ruan, L., Xiong, R., Crandall, J. and Deibert, R., 'We Chat, They Watch: How International Users Unwittingly Build Up WeChat's Chinese Censorship Apparatus', Citizen Lab, University of Toronto, 7 May 2020. Available at: https://citizenlab.ca/2020/05/we-chat-they-watch

Kosta, E., 'Algorithmic state surveillance: Challenging the notion of agency in human rights', Regulation & Governance, 7 July 2020. Available at: https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12331

Kostka, G., 'China's social credit systems and public opinion: Explaining high levels of approval', New Media & Society, 27(7), 2019. Available at: https://journals.sagepub.com/doi/full/10.1177/1461444819826402

Llanso, E., van Hoboken, J., Leerssen, P. and Harambam, J., 'Artificial Intelligence, Content Moderation, and Freedom of Expression', Transatlantic Working Group, 2020. Available at: www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf

MacKinnon, R., 'Chinese tech giants can change: But the state is still their number one stakeholder', 2021. Available at: https://rankingdigitalrights.org/index2020/spotlights/china-tech-giants

Maizland, L., 'China's Repression of Uyghurs in Xinjiang', Council on Foreign Relations, 1 March 2021. Available at: https://www.cfr.org/backgrounder/chinas-repression-uyghurs-xinjiang

Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A. and Deibert, R., 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', Citizen Lab Research Report No. 113, University of Toronto, 18 September 2018. Available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries

Marczak, B., Scott-Railton, J., Senft, A., Abdul Razzak, B. and Deibert, R., 'The Kingdom Came to Canada. How Saudi-Linked Digital Espionage Reached Canadian Soil', Citizen Lab, University of Toronto, 1 October 2018. Available at: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/).

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R. and Paxson, V., 'China's Great Cannon', Citizen Lab, University of Toronto, 10 April 2015. Available at: https://citizenlab.org/2015/04/chinas-great-cannon

McCarthy, O.J., 'AI & Global Governance: Turning the Tide on Crime with Predictive Policing', United Nations University - Centre for Policy Research, 26 February 2019. Available at: https://cpr.unu.edu/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html

Michaelsen, M.,' The Digital Transnational Repression Toolkit, and Its Silencing Effects', Freedom House, 2020. Available at: https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects

Mitsilegas, Valsamis, 'Responding to Covid-19. Surveillance, Trust and the Rule of Law', 2020

Mortera-Martinez, C., 'The EU's security union: a bill of health', CER, London, 21 June 2019. Available at: https://www.cer.eu/publications/archive/policy-brief/2019/eus-security-union-bill-health

Mozur, P., Kessel, J. M. and Chan M., 'Made in China, Exported to the World: The Surveillance State', New York Times, 24 April 2019. Available at: http://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Nyst, C. and Falchetta, T., 'The Right to Privacy in the Digital Age', Journal of Human Rights Practice, 9 (1), 2017. Available at: https://doi.org/10.1093/jhuman/huw026

Omer, T. and Polonetsky, J., 'Big data for all: Privacy and user control in the age of analytics', Nw. J. Tech. & Intell. Prop. 11, 2012. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/nwteintp11&div=&id=&page=

Öztürk, A. E. and Taş, H., 'The Repertoire of Extraterritorial Repression: Diasporas and Home States', Migration Letters, 17(1), 2020, 63-64. Available at: https://journals.tplondon.com/ml/article/view/853/700

Polyakova, A. and Meserole, C., 'Exporting digital authoritarianism: The Russian and Chinese models' Policy Brief, Democracy and Disorder Series, 2019. Available at: www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

Ragnedda, M., 'Social control and surveillance in the society of consumers', International Journal of Sociology and Anthropology, 3(6), 2011. Available at: www.researchgate.net/publication/228962740_Social_control_and_surveillance_in_the_society_of_consumers

Raine, S., 'Europe's Strategic Future: From Crisis to Coherence?', London, International Institute for Strategic Studies, 2019. Available at: https://www.iiss.org/publications/adelphi/2019/europes-strategic-future-from-crisis-to-coherence

Rheault, L., Rayment, E. and Musulan, A. 'Politicians in the line of fire: Incivility and the treatment of women on social media', Research & Polictics, 6(1), 2019. Available at: https://journals.sagepub.com/doi/10.1177/2053168018816228

Roberts, S.L., 'Tracking Covid-19 using big data and big tech: a digital Pandora's Box', LSE British Politics and Policy, 2020. Available at: https://blogs.lse.ac.uk/politicsandpolicy/tracking-covid-19/

Roskomnadzor, 'Социальные сети будут привлечены к ответственности за вовлечение подростков в противоправную деятельность', 27 January 2021. Available at: https://rkn.gov.ru/news/rsoc/news73328.htm

Ruan, L., Knockel, J., NG, J. Q., Crete-Hishihata, M., 'One App, Two Systems How WeChat uses one censorship policy in China and another internationally', Citizen Lab, University of Toronto, 30 November 2016. Available at: https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems

Rudnitsky,J. and Khrennikov I., 'Moscow Tightens Lockdown With Digital Permits as Virus Spreads', Bloomberg, 10 April 2020. Available at: http://www.bloomberg.com/news/articles/2020-04-10/moscow-tightens-lockdown-with-permit-system-as-virus-spreads

Rydzak, J., 'Disconnected: A human rights-based approach to network shutdowns', Global Network Initiative, 2018. Available at: https://globalnetworkinitiative.org/wpcontent/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf

Rydzak, J., Karanja, M. and Opiyo, N., 'Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries', International Journal of Communication, 14(2020), 2020. Available at: https://ijoc.org/index.php/ijoc/article/view/12770/3185

Sætra, H.S., 'A shallow defence of a technocracy of artificial intelligence: Examining the political harms of algorithmic governance in the domain of government', Technology in Society, 2020. Available at: www.sciencedirect.com/science/article/pii/S0160791X19305925

Santa Clara Principles on Transparency and Accountability in Content Moderation, 2018. Available at: https://santaclaraprinciples.org/

Schenkkan, N. and Linzer, I., 'Out of Sight, Not Out of Reach. The Global Scale and Scope of Transnational Repression', Freedom House, 2021. Available at: https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf

Shahbaz, A., Funk, A. and Hackl, A., 'User Privacy or Cyber Sovereignty?', Freedom House, 2020. Available at: https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty

Singer, N., Metz, C., 'Many Facial-Recognition Systems Are Biased, Says U.S. Study', The New York Times, 20 December 2019. Available at: www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

Smętek, J., Warso, Z., 'Cyberprzemoc wobec kobiet' ('Cyberviolence against woman'), Helsinki Foundation for Human Rights, 2017. Available at: www.hfhr.pl/wp-content/uploads/2017/12/HFPC-Cyberprzemoc-wobec-kobiet-raport-www.pdf

Stanley, J. and Granick, J. S., 'The limits of location tracking in an epidemic', American Civil Liberties Union, 2020. Available at: www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf

Stanley, Jay and Granick, Jennifer S., 'The limits of location tracking in an epidemic', American Civil Liberties Union, 2020

T. Ginsburg (2020), 'How Authoritarians Use International Law', Journal of Democracy, Vol. 31 Issue 4.

Ulmer, A. and Siddiqui Z., 'India's use of facial recognition tech during protests causes stir', Reuters, 17 February 2020. Available at: www.reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ

von Ow-Freytag, B., 'Filling the void: why the EU must step up support to Russian civil society', Martens Centre for European Studies, 2018. Available at: https://journals.sagepub.com/doi/full/10.1177/1781685818813294

Wagner, B., Bronowicka, J., Berger, C. and Behrndt, T., 'Surveillance and censorship: the impact of digital technologies on human rights', European Parliament, 16 April 2015. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_STU%282015%29549034

Wang, V., 'Chinese Citizen Journalist Sentenced to 4 Years for Covid Reporting', The New York Times, 28 December 2020. Available at: www.nytimes.com/2020/12/28/world/asia/china-Zhang-Zhan-covid-convicted.html

Wood, D.M. and Ball, K., (eds), 'A report on the surveillance society', Surveillance Studies Network, UK, 2006. Available at: https://vcut.org/a_report_on_the_surveillance.pdf

Wu, W., Huang, T. and Gong, K., 'Ethical Principles and Governance Technology Development of AI in China', Engineering, 6(3), March 2020. Available at: www.sciencedirect.com/science/article/abs/pii/S2095809920300011

Youngs, R., 'The EU's Global Human Rights Sanctions regime: Breakthrough or Distraction?', Carnegie Europe, December 2020.

Zamfir, I., 'Democracy support in EU external policy', European Parliament Research Service Briefing, 2018.

Ziv, A., 'This Israeli face-recognition startup is secretly tracking Palestinians', Haaretz, 15 July 2019. Available at: www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359

Zuboff, S., 'The age of surveillance capitalism: The fight for a human future at the new frontier', New York: Public Affairs, 2019.

Zuiderveen Borgesius, F., 'Discrimination, artificial intelligence, and algorithmic decision-making', Council of Europe, 2018. Available at: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

## Non-governmental organisations, media and joint publications

Access Now, '#KeepItOn: Open letter appealing to the Deputy Director-General to urge the governments of Bangladesh, India, Myanmar, and Pakistan to end the ongoing internet shutdown amid COVID-19 pandemic', 26 May 2020. Available at: www.accessnow.org/civil-society-to-who-lets-end-government-ordered-internet-shutdowns

Access Now, 'A closer look at China's Cybersecurity Law - cybersecurity, or something else?', 13 December 2017. Available at: https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/

Access Now, 'A digital rights agenda for 2021 and beyond', 18 August 2020. Available at: www.accessnow.org/a-digital-rights-agenda-for-2021-and-beyond/

Access Now, 'Cutting internet access when people need it the most: stories from Uganda', 9 February 2021. Available at: https://www.accessnow.org/internet-shutdown-stories-from-uganda/

Access Now, 'Ethiopia: Communications Shutdown Takes Heavy Toll', 9 March 2020. Available at: www.hrw.org/news/2020/03/09/ethiopia-communications-shutdown-takes-heavy-toll

Access Now, 'Internet censorship in Tanzania: the price of free expression online keeps getting higher', 20 October 2020. Available at: www.accessnow.org/internet-censorship-in-tanzania

Access Now, 'Keep It On Report 2018', 2019. Available at: www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf

Access Now, 'Keep It On Report 2019', 2020. Available at: www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

Access Now, 'Rights groups to Facebook on Tunisia's "disappeared" accounts: we're still waiting for answers', 23 June 2020. Available at: https://www.accessnow.org/rights-groups-to-facebook-on-tunisias-disappeared-accounts-were-still-waiting-for-answers

Access Now, Article 19, Association for Progressive Communications (APC), Chinese Human Rights Defenders, CIVICUS, International Service for Human Rights, Ranking Digital Rights, Safeguard Defenders, 'Joint civil society open letter to the UN on public-private partnerships', 2020. Available at: https://www.apc.org/en/pubs/joint-civil-society-open-letter-un-public-private-partnerships

Ada Lovelace Institute, 'Exit Through The App Store', 2020. Available at: www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf

Amnesty International and Access Now, 'The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems', 2018. Available at: https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf

Amnesty International, 'Amnesty reveals alarming impact of online abuse against women', 2017. Available at: www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women

Amnesty International, 'NSO Group spyware used against Moroccan journalist days after company pledged to respect human rights', 22 June 2020. Available at: http://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist

Amnesty International, 'Out of Control: Failing EU Laws for Digital Surveillance Export', London, 2020. Available at: https://www.amnesty.org/en/documents/EUR01/2556/2020/en/

Article 19, 'Investigating online harassment and abuse of women journalists', 2020. Available at: (www.article19.org/wp-content/uploads/2020/11/Gender-Paper-Brief-3-.pdf

Association for Progressive Communications and other NGOs, 'Ecuador: Surveillance technologies implemented to confront COVID-19 must not endanger human rights', 19 March 2020. Available at: http://www.apc.org/en/pubs/ecuador-surveillance-technologies-implemented-confront-covid-19-must-not-endanger-human-rights

BBC, 'Myanmar coup: Military blocks Facebook for ake of stability', 5 February 2021. Available at: http://www.bbc.com/news/world-asia-55923486

BBC, 'Russia: Moscow uses facial recognition to enforce quarantine', 3 April 2020. Available at: www.bbc.com/news/av/world-europe-52157131

B-Tech Project. Available at: http://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx

Business and Human Rights Resource Centre, 'Human rights due diligence within the tech sector: developments and challenges', 1 December 2020. Available at: https://www.business-humanrights.org/en/blog/human-rights-due-diligence-within-the-tech-sector-developments-and-challenges/

CISA, 'Understanding Denial-of-Service Attacks', November 20 2019

Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 'State of internet freedom in Africa. Resetting Digital Rights Amidst The Covid-19 Fallout', 2020. p. 6. Available at: https://cipesa.org/2020/09/report-the-state-of-internet-freedom-in-africa-2020/

Digital Freedom Fund. Available at: https://digitalfreedomfund.org/

European Endowment for Democracy (EED), 'Annual Report 2018: Supporting People Striving for Democracy', Brussels. 2018. Available at: https://www.euneighbours.eu/en/south/stay-informed/publications/european-endowment-democracy-annual-report-2018-supporting-people

European Partnership for Democracy, 'Louder than words? Connecting the dots of European democracy support', Brussels: EPD, 2019. Available at: https://epd.eu/2019/09/30/louder-than-words-connecting-the-dots-of-european-democracy-support/

Financial Times, 'EU pressured to give results of leak probe on China disinformation', 21 June 2020. Available at: https://www.ft.com/content/5a323cec-82a6-4e64-9bbb-27e8de7b9929

Freedom House, 'COVID-19 Censorship and Surveillance Data'. Available at: https://freedomhouse.org/sites/default/files/2020-10/10082020_COVID-19_Censorship_and_Surveillance_Data_Updated.xlsx

Freedom House, 'Freedom of the Net Report 2020', 2020. Available at: https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow

Freedom House, 'Freedom of the Net. 2018', 2018. Available at: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Freedom House, 'Freedom of the Net. 2020. China country report', 2020. Available at: https://freedomhouse.org/country/china/freedom-net/2020#C

Freedom Online Coalition. Available at: www.freedomonlinecoalition.com

Global coalition of more than 300 civil society organisations, 'Global call for international human rights monitoring mechanisms on China. An open letter to: UN Secretary-General Antonio Guterres, UN High Commissioner for Human Rights Michelle Bachelet, UN Member States', 2020. Available at: http://www.hrw.org/news/2020/09/09/global-coalition-urges-un-address-chinas-human-rights-abuses

Human Rights Watch, 'Bangladesh: Internet blackout on Rohinya Refugees', 13 September 2019. Available at: http://www.hrw.org/news/2019/09/13/bangladesh-internet-blackout-rohingya-refugees

Human Rights Watch, 'China's Global Threat to Human Rights', 2020. Available at: www.hrw.org/world-report/2020/country-chapters/global

Human Rights Watch, 'Ecuador: Privacy at Risk with Covid-19 Surveillance', 1 July 2020. Available at: www.hrw.org/news/2020/07/01/ecuador-privacy-risk-covid-19-surveillance

Human Rights Watch, 'End Internet Shutdowns to Manage COVID-19', 31 March 2020. Available at: www.hrw.org/news/2020/03/31/end-internet-shutdowns-manage-covid-19

Human Rights Watch, 'End Internet Shutdowns to Manage COVID-19', 31 March 2020. Available at: www.hrw.org/news/2020/03/31/end-internet-shutdowns-manage-covid-19

Human Rights Watch, 'Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights', 15 November 2019. Available at: www.hrw.org/news/2019/11/15/facial-recognition-deal-kyrgyzstan-poses-risks-rights

Human Rights Watch, 'Joint Statement on Russia's 'Sovereign Internet Bill', 24 April 2019. Available at: www.hrw.org/news/2019/04/24/joint-statement-russias-sovereign-internet-bill

Human Rights Watch, 'Rules for a New Surveillance Reality', 18 November 2019. Available at: www.hrw.org/news/2019/11/18/rules-new-surveillance-reality

Human Rights Watch, 'Russia: Health Workers Face Retaliation for Speaking Out', 15 June 2020. Available at: www.hrw.org/news/2020/06/15/russia-health-workers-face-retaliation-speaking-out

Human Rights Watch, 'Russia: New Law Expands Government Control Online', 31 October 2019. Available at: www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online

Human Rights Watch, 'Russia: Social Media Pressured to Censor Posts', 5 February 2021. Available at: http://www.hrw.org/news/2021/02/05/russia-social-media-pressured-censor-posts

Human Rights Watch, 'Turkey: Probes Over Doctors' Covid-19 Comments', 10 June 2020. Available at: www.hrw.org/news/2020/06/10/turkey-probes-over-doctors-covid-19-comments

Human Rights Watch, 'Ukraine: Trapped in a War Zona for Lacking a Smartphone', 26 June 2020. Available at: www.hrw.org/news/2020/06/26/ukraine-trapped-war-zone-lacking-smartphone

Human Rights Watch, 'Venezuela: A Police State Lashes Out Amid Covid-19', 28 August 2020. Available at: www.hrw.org/news/2020/08/28/venezuela-police-state-lashes-out-amid-covid-19

Human Rights Watch, 'Video Unavailable. Social Media Platforms Remove Evidence of War Crimes', 10 September 2020. Available at: https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes

Human Rights Watch, 'Russia', 2020. Available at: https://www.hrw.org/europe/central-asia/russia

ICFJ, 'ICFJ-UNESCO Global Study: Online Violence Against Women Journalists', 2020

Internet Governance Forum. Available at: www.intgovforum.org

Internet Society, 'Internet Society Perspectives on Internet Content Blocking: An Overview', 2017. Available at: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

Internet Society, 'Policy Brief: Internet Shutdowns', 2019. Available at: www.internetsociety.org/policybriefs/internet-shutdowns#_edn34

Join letter of several human rights NGOs, 'Restrictions on Communication, Fencing, and COVID-19 in Cox's Bazar District Rohingya Refugee Camps', 2 April 2020. Available at: https://www.fortifyrights.org/downloads/Joint%20Letter%20-%20Restrictions%20on%20Communication,%20Fencing,%20and%20COVID-19%20in%20Cox%E2%80%99s%20Bazar%20District%20Rohingya%20Refugee%20Camps.pdf

Joint civil society statement, 'States use of digital surveillance technologies to fight pandemic must respect human rights', 2020. Available at: http://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf

Netblocks, 'Internet disrupted in Russia amid opposition protests', 23 January 2021. Available at: https://netblocks.org/reports/internet-disrupted-in-russia-amid-opposition-protests-98aRXQAo

Open Government Partnership, 'A Guide to A Guide to Open Government and the Coronavirus: Privacy Protections', 2020. Available at: https://www.opengovpartnership.org/documents/a-guide-to-open-government-and-the-coronavirus-privacy-protections/

Politico, 'EU to limit export of 'sensitive' tech in response to Hong Kong security law', 28 July 2020. Available at: https://www.politico.eu/article/eu-to-limit-export-of-sensitive-tech-in-response-to-hong-kong-security-law/

Privacy International, 'Public-Private surveillance partnerships', 2020. Available at: https://privacyinternational.org/learn/public-private-surveillance-partnerships

Privacy International, 'Singapore contact tracing app made mandatory for migrant workers', 2020. Available at: https://privacyinternational.org/examples/3890/singapore-contact-tracing-app-made-mandatory-migrant-workers

Privacy International, 'Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes', 10 November 2020. Available at: https://privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes

Privacy International, 'The Global Surveillance Industry', 2016. Available at: https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

Privacy International, 'Tracking Global responses to Covid-19',2020. Available at: https://privacyinternational.org/examples/tracking-global-response-covid-19

Ranking Digital Rights, 'Ranking Digital Rights Corporate Accountability Index 2020', 2021. Available at: https://rankingdigitalrights.org/index2020

Ranking Digital Rights, 'The RDR Index 2019', 2019. Available at: https://rankingdigitalrights.org/index2019/report/freedom-of-expression

RBC, 'European Commission promises mandatory due diligence legislation in 2021', 2020. Available at:https://responsiblebusinessconduct.eu/wp/2020/04/30/Commission%20concerning%20mandatory%20due%20diligence%20for%20companieeuropean-commission-promises-mandatory-due-diligence-legislation-in-2021/

Reporters Without Borders, 'Round -up 2020. Journalists detained, held hostage and missing', 2020. Available at: https://rsf.org/sites/default/files/rsfs_2020_round-up_0.pdf

Reporters Without Borders, 'RSF unveils 20/2020 list of press freedom's digital predators', 10 March 2020. Available at: https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators

Reuters, 'EU's Borrell accuses Russia of spreading COVID-19 disinformation to sell its vaccine', 28 December 2020. Available at: https://www.reuters.com/article/health-coronavirus-eu-russia/eus-borrell-accuses-russia-of-spreading-covid-19-disinformation-to-sell-its-vaccine-idUSL8N2J81IG

Shift and the Institute for Human Rights and Business, 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', European Commission. Available at: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf

The Guardian, 'EU says China behind huge wave of Covid-19 disinformation', 10 June 2020. Available at: https://www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign

The National, 'Coronavirus: Bahrain to use electronic tags for people in quarantine', 5 April 2020. Available at: http://www.thenationalnews.com/world/gcc/coronavirus-bahrain-to-use-electronic-tags-for-people-in-quarantine-1.1001903

York, J. C., 'The Santa Clara Principles During COVID-19: More important than ever', Electronic Frontier Foundation, 2020.

# List of consulted stakeholders

| No. | Date | Interviewee |
|---|---|---|
| 1. | 24.11.2020 | Interview with key informant, under full anonymity |
| 2. | 26.11.2020 | Interview with key informant, under full anonymity |
| 3. | 27.11.2020 | Interview with four representatives of EU institution |
| 4. | 02.12.2020 | Interview with a representative of EU institution |
| 5. | 02.12.2020 | Interview with two representatives of the EEAS |
| 6. | 03.12.2020 | Interview with three key informants, under full anonymity |
| 7. | 09.12.2020 | Interview with Juan Carlos Lara, Research and Policy Director, Derechos Digitales |
| 8. | 09.12.2020 | Interview with a representative of EU institution |
| 9. | 15.12.2020 | Interview with a representative of EU institution |
| 10. | 17.12.2020 | Interview with Jonathan McCully, Legal Adviser, Digital Freedom Fund |
| 11. | 17.12.2020 | Interview with a representative of EU institution |
| 12. | 22.12.2020 | Interview with a representative of the European Endowment for Democracy |
| 13. | 06.01.2021 | Interview with Gaspar Pisanu, Latin America Policy Manager, Access Now |
| 14. | 08.01.2021 | Interview with Diego Naranjo, Head of policy, European Digital Rights |
| 15. | 08.01.2021 | Interview with Patrick Penninckx, Head of the Information Society Department of the Council of Europe |
| 16. | 14.01.2021 | Interview with a representative of an international institution |
| 17. | 20.01.2021 | Interview with private sector representative |
| 18. | 29.01.2021 | Online written consultation with a representative of EU institution |
| 19. | 12.03.2021 | Interview with a representative of EU institution |

# Annex 2: Research tools

## Interview topic guide – EU institutions

**The study "Digital technologies as a means of repression and social control - options for the EU's external human rights policy" for the European Parliament (EP/EXPO/DROI/FWC/2019-01/LOT6/R/04)**

**INTERVIEW TOPIC GUIDE**

**(AND REPORT TEMPLATE)**

EU institutions version

***Instructions for the interviewer:***

*Before the interview:*

- Familiarise yourself with the legal mandate of the interviewee's institution and the responsibilities of the interviewee's specific unit/department vis-à-vis EU foreign policy.

*Immediately before beginning the interview:*

- Confirm whether the interviewee agrees to the interview.
- Determine whether and how the interviewee would like to be quoted in the final paper:
    - ☐ Full citation with name and organisational affiliation;
    - ☐ Citation of only my position and organisational affiliation;
    - ☐ Citation of only my organisational affiliation; or
    - ☐ Citation only in terms of sector (i.e. representative of EU institution etc.).
- Ask for permission for recording and explain that recording is voluntary and only for internal purposes to prepare write-ups from interviews.
- Once recording is switched on, confirm that the consent for recording was obtained.
- Explain to the interviewee that the study relates to the problem of using digital technologies for repression and social control. Clarify that its main purposes are to: (1) provide an overview of the international HR framework which is relevant to this phenomenon and (2) describe and assess relevant EU foreign policy framework and toolbox with the view to its effectiveness and completeness, as well as available expertise and resources. Underline that in the interview, we will concentrate on obtaining better understanding of the options that the EU has in its foreign policy

toolbox to address such use of digital technologies and learning how effective the toolbox is in practice.

- **It should also be made very clear that the study is only about human rights impacts in third countries.** This is important because with the discussion about foreign disinformation (which is partly based on the use of digital technologies), foreign policy tools are also used to address human rights impacts within the EU and its MS.

**Part 1. Use of digital technologies for repression and social control**

1. Have you noted, as part of your work, instanced when digital technologies were used by the authorities in third countries for repression and social control?
2. *(if YES to Q1, and based on the interviewee's professional experience)* What are some of the new and emerging digital technologies that have the most significant impact on human rights? How are these technologies used for repression and social control?
3. *(if YES to Q1, and based on the interviewee's professional experience)* From the EU perspective, what are the key human rights challenges arising from the use of digital technologies?

**Part 2. Interviewee's involvement in EU foreign policy**

4. Could you briefly explain your role within your institution? (What is your area of responsibility in relation to EU foreign policy?) (*if not addressed earlier, or to confirm understanding – then rephrase appropriately*)
5. What EU policy instruments do you work with? (alternative: What is your mandate vis-à-vis specific instruments?) (*if not addressed earlier, or to confirm understanding – then rephrase appropriately*)
6. Could you briefly explain how you work with those instruments? What does it look like in practice/on the ground? (*if not addressed earlier, or to confirm understanding – then rephrase appropriately*)

**Part 3. EU instruments responsive to the abuse of digital technologies**

7. Which, if any, EU foreign policy tools that you have experience with (at the disposal of your institution) allow the EU (in one way or another) to address /respond to the use of digital technologies for repression and social control?
8. How can these instruments be used to tackle the use of digital technologies for repression and social control? *(if not addressed earlier, or to confirm understanding – then rephrase appropriately)*
9. Do you recall any instances when specific foreign policy instruments were applied to tackle the use of digital technologies for repression and social control? Could you describe some examples?

**Part 4. Effectiveness of EU foreign policy instruments in tackling the use of digital technologies for repression and social control**

10. *(If YES to Q9)* To what extent does the application of the EU foreign policy instruments that you have at your disposal contribute to limiting the use of digital technologies for repression and social control or to limiting the impact of such use on targeted people/communities?

a. In situation that you recalled earlier (under Q9), how did the applied measures work in practice? Was there any change in response to their application?

b. From the perspective of tackling the use of digital technologies for repression and social control, what are the strengths and weaknesses of specific tools/instruments that you work with?

11. Are you able to determine which measures (or combinations of measures) have more impact on the practices in third countries? (i.e. better help to limit/curb the use of digital technologies for repression and social control)

12. In your view, what factors influence (or can influence) the effectiveness of applied EU foreign policy tools?

13. What conditions help to increase the effectiveness of EU foreign policy tools?

**Part 5. Comprehensiveness of EU foreign policy instruments in tackling the use of digital technologies for repression and social control**

14. Does the EU foreign policy toolbox allow the EU to properly tackle all instances when digital technologies are used for repression and social control?

c. *(If YES to Q13)* Would you then say that the instruments are used to their full potential at the moment? If NOT, why? What should change in the practical application of those instruments?

d. *(If NO to Q13)* Why not? Are there any instruments/solutions missing? What are those missing instruments/solutions? Can you recall any tools that were put forward in the past, but did not materialise/did not get adopted? Why?

**Part 5. Available resources and expertise**

15. *(in the context of dynamically developing digital technologies)* What is your assessment of the resources and expertise within your institution to properly respond – using the available EU foreign policy tools – to the use of digital technologies for repression and social control?

**Part 6. International/regional HR framework**

16. In your view, can the existing international or regional human rights framework address the problem of digital technologies being used as means of repression and social control?

e. Is the framework sufficient? If NO, what is missing?

f. What can the EU do to improve this framework?

17. Is there anything you would like to add before we finalise the interview?

**The study "Digital technologies as a means of repression and social control - options for the EU's external human rights policy" for the European Parliament (EP/EXPO/DROI/FWC/2019-01/LOT6/R/04)**

# INTERVIEW TOPIC GUIDE

# (AND REPORT TEMPLATE)

CSOs & other respondents version

***Instructions for the interviewer:***

*Immediately before beginning the interview:*

- Confirm whether the interviewee agrees to the interview.
- Determine whether and how the interviewee would like to be quoted in the final paper:
    - ☐ Full citation with name and organisational affiliation;
    - ☐ Citation of only my position and organisational affiliation;
    - ☐ Citation of only my organisational affiliation; or
    - ☐ Citation only in terms of sector (i.e. representative of EU institution etc.).
- Ask for permission for recording and explain that recording is voluntary and only for internal purposes to prepare write-ups from interviews.
- Once recording is switched on, confirm that the consent for recording was obtained.
- Explain to the interviewee that the study relates to the problem of using digital technologies for repression and social control. Clarify that its main purposes are to: (1) provide an overview of the international HR framework which is relevant to this phenomenon and (2) describe and assess relevant EU foreign policy framework and toolbox with the view to its effectiveness and completeness, as well as available expertise and resources. Underline that in the interview, we will concentrate on obtaining better understanding of the options that the EU has in its foreign policy toolbox to address such use of digital technologies and learning how effective the toolbox is in practice.

**Trends in the use of new technologies for repression and social control**

1. What are new and emerging digital technologies that have the most significant impact on human rights (in the context of repressions or/and social control) in the recent years, used globally or/and in the region where you work? What are the key human rights challenges arising from the use of

those technologies? Is there anything in particular that makes today's digital technologies different from earlier periods?

2. Could you give at least one example of the application of such technologies (in particular in the region where you work)?
3. Do you observe any other trends/phenomena in actions taken by state actors in relation to new technologies that have negative implications for human rights globally/in the region where you work (such as export/import of new technologies that are then used for widespread surveillance, internet shutdowns, extending surveillance powers of state agencies by legislation etc.)? Please provide concrete examples to the extent possible.
4. What (which countries) are the global/regional "leaders" in using new technologies (and/or setting/applying the above-mentioned trends) in a way that may challenge human rights? Please justify your choice.
5. Are there any particular groups most vulnerable to the negative impact of those actions? (racial, gender, religious, social, political etc.)
6. What is the role of private actors in this context? Which categories of private actors are particularly critical? (e.g. internet platforms, companies producing surveillance technologies) Could you give examples?
7. What is the impact of the COVID-19 pandemic on the use of new technologies that may have negative implications for human rights (in particular in the region where you work)?
8. Have there been any other particular events (protests, elections etc.) in the recent years which triggered an increased use of new technologies with negative implications for human rights in the region where you work?
9. Could you point us towards the recent key publications/accomplishments/other developments of your organization on the issue of new digital technologies and human rights?

**International HR legal framework**

10. What is your general assessment of the current international HR legal framework related to the use of new digital technologies? Is it adequate and effective in addressing human rights challenges posed by those technologies?
11. Can you observe any particular trends in how HR systems have been responding in the recent years (or may respond in the near future) to the challenges related to the use of new digital technologies for repression and social control?
12. What are the major problems or gaps in the current HR legal framework (such as important technologies/areas that have been overlooked or that need to be further addressed or standards that are inadequate or insufficient in the context of actual challenges)?
13. What are the most important issues that should be considered on the current agendas of the international HR bodies? What types of reforms are needed to improve the existing HR legal framework?
14. Do you observe any particular clashes/discrepancies between different HR systems (universal vs. regional, different regional ones) regarding the use of new technologies?
15. Can you identify any examples of particularly important developments/good practices undertaken by international HR bodies in the context of risks arising from new digital technologies?

16. What is your assessment of the current HR legal framework as far as human rights obligations of private actors in the technological field are concerned? Are they comprehensive, sufficient and effective?
17. What is your assessment of the responses of the different international HR systems to the COVID-19 crisis? Does the pandemic affect the ways in which international HR standards should apply to tech companies?
18. Is there anything else that you would like to add?

PE 653.636
EP/EXPO/DROI/FWC/2019-01/LOT6/R/04

Print ISBN 978-92-846-8025-2 | doi:10.2861/6706 | QA-05-21-111-EN-C
PDF ISBN 978-92-846-8024-5 | doi:10.2861/953192 | QA-05-21-111-EN-N