



Global Campus
of Human Rights

Volume 3 No 2
2019

Global Campus Human Rights Journal



Editorial committee

Frans Viljoen
Convening editor
University of Pretoria

Mike Hayes
Co-editor
Mahidol University

Veronica Gomez
Co-editor
University of San Martin

Diego Lopez
Co-editor
University of San Martin

Editorial assistant

Isabeau de Meyer
University of Pretoria

International editorial advisory board

Juan Pablo Alban
Universidad San Francisco de Quito, Ecuador

Marco Borraccetti
University of Bologna

Vahan Bournazian
Yerevan State University

Nancy Cardinaux
University of Buenos Aires

Mudar Kassis
Birzeit University, Palestine

Asim Mujkic
University of Sarajevo

Esther Damalie Naggita-Musoke
Makerere University

Gerd Oberleitner
University of Graz

Sriprapha Petcharamesree
Mahidol University

Geeta Sangroula
Kathmandu School of Law, Nepal

The *Global Campus Human Rights Journal (GCHRJ)* is a peer-reviewed scholarly journal, published under the auspices of the Global Campus of Human Rights (see <https://gchumanrights.org/research/publications/global-campus-human-rights-journal.html>) as an open-access on-line journal. It is supported financially by the European Union Commission and appears twice annually.

This journal should be cited as (2019) 3 *Global Campus Human Rights Journal*

ISSN: 2532-1455

Headquarters and contact information:

Global Campus of Human Rights
Monastery of San Nicolò, Riviera San Nicolò, 26 I-30126 Venice Lido, Italy
<https://gchumanrights.org>



This journal content is offered under a [CC Attribution Non-Commercial No Derivatives](https://creativecommons.org/licenses/by-nc-nd/4.0/) license. Content in this journal can be considered under this license unless otherwise noted.

Global Campus Human Rights Journal

Volume 3 No 2 2019

**Global Campus of Human Rights
2020**

The *Global Campus Human Rights Journal* (GCHRJ) is a peer-reviewed scholarly journal, published under the auspices of the Global Campus of Human Rights as an open-access on-line journal.

Aim: The *Global Campus Human Rights Journal* aims to serve as a forum for rigorous scholarly analysis, critical commentaries, and reports on recent developments pertaining to human rights and democratisation globally, particularly by adopting multi- and inter-disciplinary perspectives, and using comparative approaches. It also aims to serve as a forum for fostering interdisciplinary dialogue and collaboration between stakeholders, including academics, activists in human rights and democratisation, NGOs and civil society.

Publication details: It is published under the auspices of the Global Campus of Regional Human Rights Masters (see <https://gchumanrights.org>), and is supported financially by the European Union Commission. It appears twice annually, in July and in December.

Open access: The *Global Campus Human Rights Journal* is an open-access journal. There are no access charges for readers. Users are free to read, download, copy, distribute, print, search, or link to the full texts of articles published in the journal, or use them for any other lawful purpose.

On-line: The *Global Campus Human Rights Journal* is an on-line journal. Its url is <https://gchumanrights.org/research/publications/global-campus-human-rights-journal.html>

Submissions: Submissions may be made at any time, electronically to idemeyer1@gmail.com. No fees are charged for submission or article processing. Submissions should:

- include an assurance that the article has not been published, submitted, or accepted elsewhere.
- conform to the style conventions on the journal web site.
- be concise.
- be written in UK English, or in French or Spanish. If submitted in French or Spanish, an abstract in English (of between 750 and 1000 words) has to be submitted together with the article.
- for English language style, follow the University of Oxford Style Guide (www.ox.ac.uk).
- be between 6 000 and 8 000 words in length, references included.
- (for submissions in English) include an abstract (summarising the article as a whole, including its aim, a clear description of its findings) of between 250 and 300 words. The abstract should include at least five key words.
- include a brief bibliography indicating academic qualifications and current professional position, and email contact address, as follows: Charles Ntuli; BA (Oxford), PhD (Lund); Visiting Professor, University of Sao Paolo; cntuli@uu.ac.za

Style guidelines: Detailed style guidelines are on the *Journal's* website, <https://gchumanrights.org/research/publications/global-campus-human-rights-journal.html>

Layout and typesetting: Lizette Hermann, Pretoria University Law Press (PULP), Centre for Human Rights, Faculty of Law, University of Pretoria.

The Global Campus of Human Rights

Headquarters and contact information

Global Campus of Human Rights

(Monastery of San Nicolò, Riviera San Nicolò, 26 I-30126 Venice Lido, Italy)

<https://gchumanrights.org>

The Global Campus of Human Rights is a unique network of one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes:

- European Master's in Human Rights and Democratisation (EMA)
- Master's in Human Rights and Democratisation in Africa (HRDA)
- European Master's Programme in Democracy and Human Rights in South East Europe (ERMA)
- Master's in Human Rights and Democratisation in Asia-Pacific (APMA)
- Master's in Human Rights and Democratisation in the Caucasus (CES)
- Master's in Human Rights and Democratisation in Latin American and the Caribbean (LATMA)
- Arab Master's in Democracy and Human Rights (ARMA)

These Regional Programmes offer specialised post-graduate education and training in human rights and democracy from a regional perspective, with an interdisciplinary content as well as a multiplicity of research, publications, public events and outreach activities. The Global Campus integrates the educational activities of the Regional Programmes through the exchange of lecturers, researchers and students; the joint planning of curricula for attended and online courses; the promotion of global research projects and dissemination activities; the professional development of graduates through internships in inter-governmental organisations; and the strong focus of networking through the Global Campus Alumni Association, as well as support to the alumni associations of the Regional Programmes.

The wealth of human resources connected by global and regional alliances fostered by the Global Campus and its Regional Programmes, offer remarkable tools and opportunities to promote human rights and democracy worldwide.

The Global Campus of Human Rights develops its activities thanks to the significant support and co-funding of the European Union – through the *European Instrument for Democracy and Human Rights* and its partner universities around the world. The Global Campus equally boasts many joint institutional agreements and strategic alliances with inter-governmental, governmental and non-governmental organisations at the local, national and international level.



Global Campus
of Human Rights

Europe
South-East Europe
Latin America-
Caribbean

Asia-Pacific
Caucasus
Arab World
Africa

Volume 3 No 2 (2019)

<https://doi.org/20.500.11825/1585>

Contents

Editorial	vii
------------------------	-----

<https://doi.org/20.500.11825/1584>

Special focus: The impact of new technologies on human rights

Editorial of special focus: The impact of new technologies on human rights.....	ix
---	----

by Diego Lopez & Veronica Gomez

<https://doi.org/20.500.11825/1583>

The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development Africa.....	147
--	-----

by Deborah Mburu Nyokabi, Naa Diallo, Nozizwe W Ntesang, Thomas Kagiso White & Tomiwa Ilori

<https://doi.org/20.500.11825/1582>

Are smart walls smart solutions? The impact of technologically-charged borders on human rights in Europe.....	173
---	-----

by Bronagh Kieran, Fuensanta Amoros Cascales, Laura Thomi & Meredith Veit

<https://doi.org/20.500.11825/1580>

Online assemblies between freedom and order: Practices in South-East Europe	210
---	-----

by Andrea Jovanović, Edo Kanlić, David Savić, Goran Stanić & Kristina Ćendić

<https://doi.org/20.500.11825/1578>

Big Brother in the Middle East and North Africa: The expansion of imported surveillance technologies and their supportive legislation	229
---	-----

by Ola El-Ashy, Ilaria Maroni, Hazem Mizyed, Razan Nammar & Mohammed Al-Maskati

<https://doi.org/20.500.11825/1577>

The impact of new information and communication technologies on the enjoyment of human rights in Latin America	250
--	-----

by Andrea Arriola, Felipe Rivadeneira, Carlos Guzman, Mailen García & Claudio Nash

<https://doi.org/20.500.11825/1576>

Dystopia is now: Digital authoritarianism and human rights in Asia	269
<i>by Mark Anthony V Ambay III, Neha Gauchan, Mahesti Hasanah & Numfon K Jaiwong</i>	
https://doi.org/20.500.11825/1575	

Sustaining human rights in the era of new technologies: Case studies of Armenia, Belarus and the Kyrgyz Republic	286
<i>by Aisuluu Abdubachaeva, Kristina Vavrik, Karen Ayvazyan, Mariam Mkrtchyan & Yuriy Nosik</i>	
https://doi.org/20.500.11825/1574	

Recent regional developments

Selected developments in human rights and democracy in 2018: Migration and asylum in Europe.....	312
<i>by Lorenzo Durante Viola, Cristina Pugnale, Federica Russo, Tamara Siwczyk & Paloma Torres Lopez</i>	
https://doi.org/20.500.11825/1573	

Selected developments in human rights and democratisation during 2018: Could it have been worse? Mixed messages for democracy and human rights in the Asia Pacific.....	337
<i>by Ravi Prakash Vyas, Mike Hayes, Nanang Indra Kurniawan & Longgina Novadona Bayo</i>	
https://doi.org/20.500.11825/1572	

Child protection and EU cooperation between Eastern Partnership countries during 2018, with a focus on Armenia, Georgia and Ukraine.....	354
<i>by Mariam Muradyan</i>	
https://doi.org/20.500.11825/1571	

Recent developments in sub-Saharan Africa during 2018	375
<i>by Ashwanee Budoo, Adem Abebe, Stephen Buabeng-Baidoo & Henok Ashagrey</i>	
https://doi.org/20.500.11825/1570	

Democracy and human rights developments in South East Europe during 2018.....	393
<i>by Odeta Berberi</i>	
https://doi.org/20.500.11825/1569	

Editorial

The first volume of the *Global Campus Human Rights Journal* appeared in 2017. This is thus the fifth issue of the *Global Campus Human Rights Journal*.

This volume consists of two parts.

The first part provides a special focus on 'technology and human rights', an area of growing interest and concern. In seven articles devoted to this topic, authors from across the globe investigate this issue. These seven articles are based on papers that were presented at an event of the Global Campus of Human Rights at which students, lecturers and other scholars interrogated the topic 'The impact of new technologies on human rights'. The Global Campus of Human Rights consists of the Global Campus Europe, South East Europe, Africa, Asia Pacific, Caucasus, Latin America and the Arab World, with the participation of post-graduate students from their respective Master's programmes in Human Rights and Democracy.

The Centre of International Studies of the University of San Martin (CIEP-UNSAM), which headquarters the Global Campus Latin American programme, in May 2019 hosted the 2019 'Global Classroom' in Buenos Aires, Argentina. Experts and representatives from governmental, inter-governmental and non-governmental agencies and organisations, including the Regional Office of the UN High Commissioner for Human Rights, UNESCO, ILO, the Delegation of the European Union in Buenos Aires and the UN Rapporteur on the Right to Privacy attended the event. The editors of this 'special focus' part of the *Journal*, Veronica Gomez, Director for Education Global Campus Latin America, and Diego Lopez, Academic Coordinator Global Campus Latin America, also provided substantive guidance in preparing and facilitating the event.

As in earlier issues of the *Journal*, the second part of this issue of the *Journal* contains a discussion of 'recent developments' in the fields of human rights and democratisation in five of the regions covered by the Global Campus of Human Rights. In this issue, developments during 2018 in five regions are covered: Europe, the Asia Pacific, the countries making up the Eastern Partnership, sub-Saharan Africa and South East Europe.

In Europe, the ability of European institutions to respond appropriately to the challenges posed by migration and quests for asylum is examined. The authors analyse the Global Compact on Migration with respect to 'climate migrants' and 'migrants in vulnerable situations'. They also identify and discuss crucial developments in this context such the criminalisation of search and rescue NGOs, the transfer of search and rescue responsibilities to third countries, and the outsourcing of migration-related responsibilities. In the Asia Pacific, issues such as the treatment of the Rohingya by the Myanmar state and the violence of the Duterte regime in the Philippines remained of concern during 2018. The

authors also shine a light on some positive developments, such as the voting out of power of the corrupt governing party in Malaysia, despite a ruling-party controlled media and various manipulations of the electoral system. A review of developments during 2018 in the Eastern Partnership reveals an ambiguous picture of both achievements and perplexing challenges. In particular, the authors deal with human rights with the focus on child protection in three selected countries: Armenia, Georgia and Ukraine. The article focuses on changes in political transformation both in domestic and international relations, economic declines and social transformations caused by the aftermath of the conflicts with Russia, as well as the advancements in fulfilling the bilateral agendas. The contribution dealing with the status of human rights and democratisation in sub-Saharan Africa discusses the African Continental Free Trade Agreement, adopted in 2018, and consider whether it can lead to more democratic governance and respect for the rule of law in African countries. It also focuses on developments within the three main African Union human rights bodies: the African Commission on Human and Peoples' Rights, the African Court on Human and Peoples' Rights and the African Committee of Experts on the Rights and Welfare of the Child.

Editorial of special focus: The impact of new technologies on human rights

Diego Lopez and Veronica Gomez***

The profusion of new technologies and of information and communication technologies in many aspects of individual and collective life is one of the defining features of our times. The advancement of new technologies in the twenty-first century – also known as the fourth industrial revolution – along with the expansion of the internet, social media and artificial intelligence has a direct impact on the way in which the public and private sectors and individuals interact. These new and transformational environments present opportunities and challenges when their practices are analysed in terms of rights.

The nature and speed of these developments have raised important questions. Among these is the impact of new technologies on the traditional notions of sovereignty and the new challenge of digital sovereignty; their impact on the dynamics of democracy and government; the challenges regarding human rights protection systems with respect to non-state actors in the realm of new technologies; the transformation of labour forces, social production relations and markets (commercial, financial, and so forth); access to education and to information in terms of use, benefit, profit and development; and the impact on the social fabric in terms of communicational dynamics, consumer behaviour, practices and identities (ethnicity, nationality, gender, class, religion, ideology).

During its 2019 Global Classroom,¹ the Global Campus of Human Rights regional programmes assessed the impact of new technologies on human rights and democracy by mapping and analysing regional and global trends. The conceptualisation of these challenges meant moving

* Diego Lopez, Political Science UBA, Academic Coordinator Global Campus Latin America.

** Veronica Gomez, Law UBA, LL.M Nottingham, Director for Education Global Campus Latin America.

1 The 2019 Global Classroom involved several months of research at the seven Global Campus regional headquarters located at Global Campus Europe, South East Europe, Africa, Asia-Pacific, Caucasus, Latin America and Arab World, with the participation of post-graduate students from their respective Master's in Human Rights and Democracy. The process culminated in a face-to-face international conference in Buenos Aires, hosted by the Centre of International Studies of the University of San Martín (CIEP-UNSAM), headquarters of Global Campus Latin America. The event, held at the Legislative Palace of the Autonomous City of Buenos Aires, was attended by experts and representatives from governmental, inter-governmental and non-governmental agencies and organisations, including the Regional Office of the UN High Commissioner for Human Rights, UNESCO, ILO, and the Delegation of the EU in Buenos Aires and the UN Rapporteur on the Right to Privacy.

away from traditional, state-centric conceptions; understanding new trends that permeate human existence in terms of the interface between technology, development and human rights; and promoting a new integrated approach to advancing development within and across nations.

The research outcomes have been summarised in the articles presented in this edition of the *Global Campus Human Rights Journal*. Each article provides a regional perspective on a particular issue and they are guided by research questions, including the identification of long-term structural challenges and at the national and regional level; the identification of actors and of conditions for the emergence of new risks to the enjoyment of rights; and the analysis of viable responses. The articles intend to understand the nexus between individual and collective rights, human development and new technologies and to analyse responses/initiatives/activities that can or should be supported when responding to the identified challenges and risks.

The contribution from Global Campus Africa (HRDA) analyses state-sponsored internet shutdowns in Zimbabwe, Sudan, Cameroon, Chad and the Democratic Republic of the Congo (DRC) in earlier 2019 coinciding with major political events, including mass protests and elections. In light of these incidents, the article addresses the role of information and communication technologies in human development and probes the intersections of the right to development and internet shutdowns in Africa. After analysing the invocation of judicial remedies in some jurisdictions and the role of the private sector in light of corporate responsibility, the article proposes a multi-stakeholder approach to face these challenges.

The contribution from Global Campus Europe reviews technological developments such as thermal imaging, biometric data, virtual reality, artificial intelligence, and drones and their deployment at the service of action at the external border of the European Union (EU) in light of the regulatory framework on data privacy in the EU and the General Data Protection Regulation (GDPR). The article explores how vulnerable groups are to be affected by the collection of biometrics, how algorithms are repositories reflecting the manufacturer's bias, and proposes a diverse workforce as a tool to face the proliferation of bias.

The contribution from Global Campus South East Europe addresses the issue of online assemblies in Croatia, Serbia, Bosnia and Herzegovina and Turkey. After exploring applicable domestic and international law, the article assesses the role of the state in providing and facilitating access to the internet and enabling online assemblies. The article analyses the surveillance of digital activities and security and its relation to online and offline assemblies.

The contribution from Global Campus Arab World analyses digital surveillance companies based in democratic countries and the use of their services by oppressive regimes, from monitoring centres facilitating mass surveillance on all telecommunications, to firewalls that filter the contents that users are allowed to access, and spyware that tap into the information stored in any personal device connected to the internet. The article assesses the volume of trade in these repression tools and the market value of surveillance companies operating in states that portrayed themselves as democracies.

The contribution from Global Campus Latin America presents a number of case studies on challenges and opportunities connected with information and communication technologies and their impact on social movements, litigation, politics and the enjoyment of individual rights. It also refers to the attempts to promote the legal regulation of the digital sphere in Colombia, Argentina and Ecuador. The analysis highlights the gap between citizens with access to technology and connectivity and those left behind.

The contribution of Global Campus Asia-Pacific focuses on digital authoritarianism as a state practice involving the invasion of privacy, the denial of access to information while promoting the spreading of misinformation, and the limitation of expression and participation. The article presents a number of case studies on arbitrary surveillance; secrecy and disinformation; fake news and misinformation, hate speech, racism and discrimination; troll armies on controlling freedom of expression and shaping public opinion; communication shutdowns; blocking and content removal by government cyber-control centres – all these leading to violations of freedom of expression – and other serious violations involving arrests, detention, gagging and killings or assassinations.

The contribution from Global Campus Caucasus aims at identifying long-term structural challenges to human rights in Armenia, Belarus and the Kyrgyz Republic with a focus on cyber security, freedom of expression, freedom of speech, access to information and data protection policies. On the one hand, the study reveals that the development of new technologies increased the accessibility of people to information in terms of e-governance programmes. Moreover, it shows that political mobilisation and participation, and freedom of expression have been enhanced due to social media developments. On the other hand, it identifies the growing challenges in terms of hate speech online, media manipulation, the spreading of disinformation, data leakage and cyber security. The piece presents a number of recommendations to stakeholders with the modernisation of legal framework as a basis, followed by unified regulations, the protection of personal data, guaranteed security in the digital environment, e-education, and culminating in the legitimate monitoring of human rights violations.

The above contributions and the general conversation leave us with the challenge of drawing equations to balance the impact of new technologies in the exercise of rights, among these the prohibition of discrimination, social rights and the access to public services, privacy and data protection, fair trial and due process, freedom of expression and freedom of assembly and association.

Editors

The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa

Deborah Mburu Nyokabi,* Naa Diallo,*
Nozizwe W Ntesang,** Thomas Kagiso White**** and
Tomiwa Ilori*****

Abstract: *The right to development is generally assessed as an all-inclusive right. It is regarded as a rallying right in which all other rights are mostly realised. The progressive nature of the right to development in realising other rights as a benchmark to a society's development has become popular even beyond legal jurisprudence to include other qualitative fields of knowledge. The role played by information and communications technology in the realisation of this right has also been acknowledged, particularly in the digital age. However, this progress has not been even across regions in the world. While some regions have experienced a fast-paced development due to ICT, several countries in Africa have been held back due to unfavourable state and non-state policies that have had negative impacts on human rights and democratic development on the continent. This article assesses the impact of ICT on the right to development, particularly as a rallying right, and the way in which the internet, a major component of ICT, has affected the right. The article especially considers the effects of network disruptions on human rights and democratic development that have become rife in the region. This study finds that there have been several human rights violations through ICT by many state and non-state actors in Africa. Most importantly, the article finds that these violations impede the right to development and pose threats to democratic development in the region. A conclusion is based on these findings and proffers feasible solutions to resolve the challenges posed by these violations.*

Key words: *right to development; Africa; information and communication technology; digital age; internet shutdowns; democratic development*

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. LLB (Hons) (Kenyatta) PGD (Kenya School of Law) LLM (Pretoria).

** MA (Ghana) MPhil (Pretoria).

*** LLB (Hons) (Botswana) LLM (Pretoria).

**** BCom (Pretoria) LLB (Hons) (Pretoria) LLM (Pretoria).

***** LLB (Hons) (Ife) BL (Lagos) LLM (Pretoria); Doctoral Researcher, Democracy, Transparency and Digital Rights Unit, Centre for Human Rights, Faculty of Law, University of Pretoria.

1 Introduction

The advent of information and communications technology (ICT) has amplified human interaction and globalisation. Therefore, human activities in all spheres of life are becoming fast-paced and redefined due to digitisation. This has also caused several developments, some of which are commendable while some, unfortunately, are undesirable (Goldsmith & Wu 2006). The internet as a major component of survival in the digital age has undergone several phases of development and over the decades many countries have been able to latch on to these developments for their socio-economic and political benefit. However, this has not been the same experience across the board, especially in many African countries. For example, of the 267 incidents of internet shutdown between 2016 and 2019, 46 have occurred in Africa (*Access Now* 2018). Several reports have linked these shutdowns to the arbitrariness of state power and very few to technical problems (CIPESA 2019). Due to the importance of the internet in the twenty-first century, not only can human development be accelerated, but democracy and human rights also have the opportunity of being improved across the world.

In the first month of 2019, and at the time of this study, five African countries had already recorded internet shutdowns. Zimbabwe, Sudan, Cameroon, Chad and the Democratic Republic of the Congo (DRC) have all experienced a shutdown at some point during this period, and the key feature of these shutdowns, as is typical of other shutdowns, is that they occur particularly when major political events such as mass protests or elections are taking place or are about to take place. These state-sponsored internet shutdowns, therefore, have been linked to the spate of democratic development in many African countries.

As a result of this connection, the article analyses the role of ICT in human development and probes the intersections of the right to development and internet shutdowns in Africa. It then considers how the right to development is being hampered by internet shutdowns on the continent and later proffers workable solutions that can address challenges posed.

2 An overview of the right to development, information communications technology and democratic development in Africa

At a global level, the right to development was regarded more as a collective right than an individual right (Villaroman 2010). It took the United Nations (UN) Declaration on the Right to Development (RTD Declaration), adopted in 1986, to formally revisit the right to development from an individual right perspective. This also in a way paved the way for more robust Global North-Global South relations as most developing countries were only beginning to rise above several decades of political instability which had caused socio-economic distress for most of these countries (Arts & Tamo 2016). This coincided with the adoption of the African Charter for Human and Peoples' Rights (African Charter) in 1981, which later entered into force a year after the RTD Declaration. To date, the African Charter in its article 22 remains the only regional framework

that imposes a duty on member states to ensure the right to development, with important cases that expand the jurisprudence of the right by the African Commission on Human and Peoples' Rights (African Commission).

The remarkable international awareness in soft law and treaties with respect to human rights, and particularly the right to development, also preceded the period when Africa experienced the third wave of democratisation – when more African countries adopted constitutional democracies and moved away from military regimes. What could be gleaned from this wave was the new constitutional culture that was the feature in most African states which caused for new institutionalised human rights systems. Some countries were able to ensure that not only civil and political rights were guaranteed, but that socio-economic rights were also protected and justiciable under these constitutions (Kibet & Fombad 2017). On civil and political rights, most constitutions began to impose term limits on public office holders, especially Presidents, and introduced more robust provisions for fundamental human rights in their constitutions (Posner & Young 2007). At least, between that period and 2018 many African countries have not only been able to invoke the constitutional limitation on term limits to force leaders from power that have exceeded their constitutionally-provided term limits, but a country such as South Africa is also regarded as one of the most improved jurisdictions in terms of socio-economic rights.

With respect to socioeconomic development, the Millennium Development Goals (MDGs), the Sustainable Development Goals (SDGs) have been regarded as an important means of achieving even development across countries. Even though the efforts of states in the implementation of SDGs vary, there is a global consensus that these goals are necessary in pushing for a more just and equitable society (Morton et al 2017). As a result, the connection between these SDGs, therefore, is tied to human rights development (Winkler & Williams 2017). Further probing this connection with respect to African countries, the right to development as defined under the African Charter states:

- (1) All peoples shall have the right to their economic, social and cultural development with due regard to their freedom and identity and in the equal enjoyment of the common heritage of mankind.
- (2) States shall have the duty, individually or collectively, to ensure the exercise of the right to development.

This provision is capable of being read outside general human rights development due to the specific mention of socio-economic rights to the exclusion of other rights. However, a close reading of the Preamble of the African Charter reveals that there is a special relationship between civil and political rights and socio-economic rights, especially as it relates to the realisation of the right to development in Africa. The African Charter points out that '[c]ivil and political rights cannot be dissociated from economic, social and cultural rights ... and that the satisfaction of economic, social, and cultural rights is a guarantee for the enjoyment of civil and political rights'.¹

1 Preamble to the ACHPR, para 8.

This settles the right to development as being not only a socio-economic right but also including civil and political rights under the African human rights system. This connection is necessary in understanding the role of ICT, as agreed to be an important aspect of human development and critical to the realisation of the right to development and the impact these have on human rights in general (Bankole et al 2001). It shows that the right to development in Africa includes the ability of citizens to access ICT for their utmost good and states' responsibility to ensure that this access is at all times guaranteed (Selian 2002). As a result, the importance of ICT in the realisation of the right to development and the right of the people to be part of such a process, including democratisation, has become an important connection to be made, especially in the digital age (Selian 2002).

As a critical and primary component in the democratisation process, the organisation of elections in Africa has played a significant role in driving democratic governments in countries such as South Africa, Senegal, Cape Verde and Mauritius. This has propelled the human rights project, particularly that of civil and political rights, because historically, the political transition in African states was a source of tensions, civil wars and military *coups* (Brown & Kaiser 2007). More recently, these elections, which in the past have been marred by violence and fraud, have been made forcefully transparent at least in the electoral process by the use of technologies (Nyabola 2018). The recently-concluded 2019 general elections in Nigeria were projected to the world by the active citizenry just as the case was in the 2015 and 2011 elections (Paradigm Initiative 2019). The same was the case in Uganda, Zimbabwe and the DRC, despite state-sponsored disruptions and attacks calculated at reducing the use of these technologies by citizens. Although the way in which digital technologies were able to play a role during these periods vary, it made the process more participatory because of the way citizen media was able to play a key role in urging political and governance audits during the elections.

These bold steps by citizens in getting more involved in the political process of their countries and also demanding more people-focused public policies may be regarded as a nuanced interpretation of the protection of the right to development. Through the enablement of ICT, many citizens have had the opportunity to demand more direct participation in governance by being able to assess power through hashtags and citizen media. What seemed to be a watershed moment for many African countries and digital technology was the Arab Spring which, through the brave act of one man, spread like wildfire across North Africa and some Middle East countries (Nyabola 2018). The effective spread of protests across the regions, made more global through the use of platforms such as Twitter, signalled the beginning of the end to a seemingly docile African citizen (Papacharissi 2014). The awakening, amplified by the internet, caused many autocratic leaders to become anxious and they have since chosen to respond in kind. Their response, together with the physical mauling of protesters and activists for more open and democratic systems, were internet shutdowns.

With Egypt also facing its fair share of the effects of the Arab Spring, it introduced a disingenuous means of stifling dissent following the footsteps of Guinea in 2007, through internet shutdowns (Ilori 2019). The importance of the internet as causing a people-focused and mass-driven

democratic development was captured by the state by the disruption of the infrastructure providing for such organisation against autocratic states. Due to the remnants of militarisation that remained in existence in most African countries despite the post-1990 constitutionalisation processes, many states also took to shutting down the internet, mainly during protests, to discourage people-centred organisations, and also during elections to assert information controls usually calculated to encourage electoral fraud and political violence (Ilori 2019).

A study recently conducted has revealed that of the 22 countries that have shut down the internet during the past five years, 77 per cent were autocratic regimes (CIPESA 2019). What this means is that there is a direct link between political underdevelopment and internet shutdowns in Africa. This has been able to link the longest-serving leaders in Africa, especially those averse to the introduction of the new features in the post-1990 constitutionalisation processes, such as Uganda, The Gambia, Egypt, DRC, Sudan and many more to the whimsical use of state powers to order internet shutdowns.

3 Conceptualising internet shutdowns

Internet shutdowns or network disruptions have been defined as ‘the intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable for a specific population within a location’ (Freyburg & Garbe 2018). Technically, the internet cannot be shut down due to its complex architecture, making the term ‘network disruption’ being preferred in some circles compared to internet shutdown. Internet shutdowns have been described as ‘the most brute force method of internet control’ (Freyburg & Garbe 2018). As explained earlier, the peculiarities of internet shutdowns in Africa have been linked to countries with records of human rights violations and protracted authoritarian practices in the region. For example, since 28 March 2018 Chad has enforced an internet shutdown lasting more than a year (Association for Progressive Communications 2019). Cameroon has also done the same due to the ongoing humanitarian crisis in the country for more than a year with huge human rights and economic costs to the country. Uganda has also at some stages carried out internet shutdowns, during either protests or general elections. In all these countries and others, the connection has been a leader who will not relinquish power and who, therefore, has grown more powerful and later fearful of the rallying power of the internet for citizens’ organisation against their rule.

The manifestation of internet shutdowns occurs and has severe effects, including preventing:

ordinary internet users from accessing any websites including social media platforms; hindering access of online mapping and coordination tools, and crippling anti-censorship tools which circumvent social media blocks such as The Onion Router (TOR) (Freyburg and Garbe 2018: 3900).

Many of the arguments against internet shutdowns have been the inability of most African countries to situate their actions within the law for legitimacy. Even though international, regional and domestic laws do not contain established sets of guidelines to engage violations of rights that occur due to the intersection of new technologies, democratic governance

and public policy, existing international law instruments have at one point or another given directions on how both state and non-state actors must approach human rights in the digital age. As will be discussed further, it has been shown that in the process of African governments shutting down the internet for justifications such as national security or public order, international law principles established through several intergovernmental and supranational bodies have held that these shutdowns occur without compliance with international human rights standards.

Together with these challenges, Africa has the most expensive mobile data in the world with users spending approximately 8,76 per cent of their monthly income to purchase one gigabyte of mobile data. This is way above the United Nations Broadband Commission recommendation of 2 per cent monthly income (Kazeem 2018). This is contrary to the principle that access to the internet should be 'affordable and available for all persons without any discrimination on any ground whatsoever', and adversely affects the right to development on the continent as envisioned in the African Declaration on Internet Rights and Freedoms (African Internet Declaration).² The lack of access in Africa due to gender inequality, the high costs of access imposed by governments, the arbitrary imposition of internet taxes and the lack of adequate infrastructure have been termed a form of censorship and impediment to the realisation of the right to development by the UN Human Rights Council (Paradigm Initiative 2017).

3.1 Justifications for internet shutdowns

There have been several justifications for internet shutdowns. Some of the prominent justifications include national security (the DRC and Uganda); elections and protests (Mali, Uganda, Ethiopia, the DRC, Chad, and Cameroon); and school examinations (Ethiopia and Algeria) (Access Now 2016). Governments are likely to enforce shutdowns 'when laws are outdated or overbroad; when laws are not transparent, and when international standards do not clearly disallow shutdowns' (Access Now 2016). The term 'national emergency' or 'national security' often is defined very broadly, resulting in the abuse of state of emergency declarations, as has been the case in Ethiopia and the Central African Republic (Access Now 2016). In Ghana, Uganda and, more recently, in Zimbabwe, governments have threatened shutdowns without making any specific reference to law, citing undefined issues such as public order, safety and destabilisation (Access Now 2019). Telecommunications regulators also oblige internet service providers to sign restrictive non-transparent contracts, which service providers cite as justification for compliance with shutdown orders (Ilori 2019).

3.2 Implications of internet shutdowns on human rights and development in Africa

Internet shutdowns are a form of technology-enabled authoritarianism and are not justifiable under international law (Ilori 2019). Internet shutdowns

2 The African Declaration on Internet Rights and Freedoms is a persuasive set of principles that looks to guide states and non-state actors in Africa on how to protect human rights in the digital age and ensure rights-respecting technology and public policy initiatives.

severely affect freedom of expression, which is a precondition for the exercise of all the other rights (*Access Now* 2016). Shutdowns are prohibited on any grounds, including national security, public order and conflict (African Declaration 2014). The Special Rapporteur on Freedom of Expression and Access to Information in Africa has bemoaned recent shutdowns in Zimbabwe, Gabon, the DRC, Sudan, and Chad and has noted that '[i]nternet and social media shutdowns violate the right to freedom of expression and access to information contrary to article 9 of the African Charter' (African Commission 2019). African governments are mandated to 'promote the establishment of the necessary conditions to foster citizen participation, transparency, access to information, freedom of the press and accountability in the management of public affairs' (African Charter 1981). African governments order internet shutdowns without complying with the standard three-part test for human rights limitations, namely, that the limitation should be anchored by law; it must be necessary in a democratic society; and it must be in pursuit of a legitimate aim (Ilori 2019). These orders by governments not only violate international law but also do great and avoidable damage to the socio-economic prospects of most of these African countries.

Internet shutdowns have been regressive for democratic development in Africa. They cause irreversible damage to political participation and freedom of expression (*Access Now* 2016). The malaise of internet shutdowns in Africa is alarming in the context of the dismal performance of sub-Saharan Africa in the Democracy Index of 2018 with only one full democracy; seven flawed democracies, 14 hybrid regimes; and 22 authoritarian regimes (CIPESA 2019). The question of whether there are political restrictions on access to the internet features in the Democracy Index survey (The Economic Intelligence Unit 2019). It is not surprising that countries that have experienced shutdowns, such as Ethiopia, Congo (Brazzaville), Cameroon, Zimbabwe, Togo, Central African Republic and the DRC, are ranked as authoritarian and have the lowest scores in the Democracy Index (The Economic Intelligence Unit 2019).

In a few exceptional cases, internet shutdowns have had the reverse effect of a surge in democratisation due to an increase in public participation. The national internet shutdown in Egypt during the Arab Spring caused street protests to spiral beyond Cairo to large sections of the population in other urban districts, suggesting that a disruption of central communication can result in unconventional local leadership of protests. In Zimbabwe, the #ShutDownZimbabwe2016 was 'the first digital campaign whereby online mobilisation resulted in offline action' (CIPESA 2019). The exceptions, however, are outliers as the impact of shutdowns on democratisation is mostly detrimental. There is a need for coordinated multi-stakeholder resistance to internet shutdowns by citizens, civil society coalitions, courts, legislators and international institutions to ensure that the dream of a democratic Africa, as envisioned by the African Charter on Democracy, Elections and Governance (African Democracy Charter), does not sink into oblivion.

Due to the lack of a go-to international instrument on a category of rights accruable in the digital age, there has been a reluctance to define new technologies, specifically the internet, as a right. Instead, the internet has been viewed as an 'enabler' of other rights (Cerf 2012). It is seen as a means of promoting already-existing rights, rather than a stand-alone right

in and of itself. This position has been shared by the United Nations General Assembly (UNGA) by stating that ‘the same rights that people have offline, must be protected online’ (General Assembly 2018). Rights accruable on the internet are regarded as not being distinctly different from the rights already provided for offline and in existing applicable international human rights law principles. This position is further cursorily considered below.

3.2.1 *The nature of internet shutdowns as violations of the right to development in Africa*

The internet has provided novel and impactful avenues for the exposure of political misbehaviour and human rights violations to internal and international audiences (Freyburg & Garbe 2018). Authoritarian governments in Africa are paranoid at the force of the internet and have resorted to using internet shutdowns as an avenue for states to assert control over digital communication and information. Since many governments get away with internet shutdowns, this emboldens other governments to resort to internet shutdowns, which are often a disproportionate mechanism of dealing with political unrest (CIPESA 2016). In countries such as Cameroon and the DRC, the governments enforced two internet disruptions within two months, showing the eagerness of governments to resort to shutdowns and how this is perceived as a go-to solution in resolving internal strife (Paradigm Initiative 2016). These shutdowns as a result are particularly egregious as they fortify access barriers on a continent that is already lagging behind in terms of access provision.

Mobile shutdown orders are often issued by national or regional judicial or executive authorities compelling internet service providers to suspend services, citing clauses in the country’s communication laws or criminal codes (Rydzak 2018). In extreme cases, verbal orders are issued by telephone followed by a written order upon demand by the internet service provider. The actual links connecting the service providers to the outside world are not terminated, but services such as specific communication applications, mobile data, SMS/texting and calls are made unavailable (Rydzak 2018). The overwhelming majority of shutdown orders target mobile networks, but a small percentage ‘entail the suspension of fixed internet access as happened in Togo in 2017’ (Rydzak 2018). Governments are often hesitant to shut down fixed lines as government offices’ operations depend on fixed and leased lines.

The technical aspects of large-scale internet shutdowns normally involve manipulating the Border Gateway Protocol (BGP), which routes the global internet traffic, by withdrawing country routes from the global routing table, as happened in Egypt when it withdrew approximately 3 500 routes accounting for 88 per cent of its internet traffic; the sabotage of infrastructure and cable cuts, which is rare as it is self-defeating for governments, but is occasionally used to justify acute disruptions, as happened in Zimbabwe in November 2017; and bandwidth throttling which is the ‘intentional slowdown of network traffic’, as happened in Gabon (Rydzak 2018; Maurushat et al 2014). A prominent feature of internet shutdowns also is that they are often bogged down by the lack of corporate or government transparency (Access Now 2016).

Given the provisions of the African Charter, the right to development, coupled with the enjoyment of civil and political rights, includes the right to work and enjoy socio-economic benefits. Internet shutdowns, however, have been shown to have had dire implications for socio-economic rights. The digital economy is projected to contribute US \$300 billion to Africa's gross domestic product (GDP) by 2025 (Ilori 2019). The repercussions of internet shutdowns are often acute due to the importance and popularity of mobile services in Africa, an industry that raised \$13 billion in taxes, generated \$110 billion in economic value, and provided 3,5 million jobs (Ilori 2019). As of 2016, 140 mobile money and banking services operated 280 million registered accounts across 39 countries including Uganda, resulting in a significant erosion of the economic rights of citizens during the internet shutdown in Uganda of 2016.

The internet offers incredible avenues, resources and innovation opportunities for a continent with the highest youth population in the world, which faces various socio-economic challenges, including unemployment (Ilori 2019). Agenda 2063 of the African Union anchors technology as a tool for the elimination of youth unemployment, guaranteeing full access to economic opportunities (AU 2063 Agenda 2013). It is estimated that shutdowns in Africa resulted in a loss of US \$237 million between 2015 and 2017 (Ilori 2019). As of February 2019, internet shutdowns had resulted in a cumulative loss of US \$267,2 million (Ilori 2016). Youth unemployment is likely to be exacerbated rather than redressed. Shutdowns undeniably put socio-economic rights at a grave irreversible risk.

3.2.2 *The violation of freedom of expression*

Article 19 of the Universal Declaration of Human Rights (Universal Declaration 1948), the foundational, but not binding, document for other human rights covenants, provides that '[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers'. It has been suggested that this article is neutral in its use of the word 'media', thereby making it possible to include the internet as a means through which one can express themselves (Joyce 2015). This notion was buttressed by a resolution passed by the Human Rights Council where the internet was included in the recognition of all forms of media (UN Human Rights Council 2016). As an improvement on the provisions of the Universal Declaration, article 19 of the International Covenant on Civil and Political Rights (ICCPR), which entered into force in 1976, amplified the provisions of freedom of expression to accommodate key but lean restrictions. Article 19 of ICCPR guarantees:

- (1) Everyone shall have the right to hold opinions without interference.
- (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
- (3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
 - (a) for respect of the rights or reputations of others;

- (b) for the protection of national security or of public order (*ordre public*), or of public health or morals.

A close reading of the provisions of the ICCPR shows that while freedom to hold an opinion is an unqualified right, freedom of expression is restricted based on certain exceptions. While these rights are not necessarily different, it may be argued that both rights can be used interchangeably and the berth afforded the right to opinion as a result can be extended to freedom of speech.

Freedom of expression as a qualified right is limited in three parts. This test provides that for the right to freedom of expression to be limited, whether offline or online, it must be provided for by law, pursue a legitimate aim and be necessary in a democratic society. These three limitative tests as restrictions on the right to freedom of expression is imposed on states under international human rights law, occur together and must be jointly satisfied. These principles enunciated by the test are further considered below.

Legality

The laws that African governments use to enforce shutdowns are not compliant with the requirements of clearly-enumerated behavioural norms as well as the limits of governmental power in enforcement. There is no delineation on the public instances in which lawful shutdown can be ordered in vague national security and emergency laws; the duration of shutdowns often is arbitrary; and the laws are silent on how long shutdowns should last. Procedurally, such laws are quickly passed without substantial input on constitutionality by legislators and the public. In *Cengiz & Others v Turkey* (Cengiz case), the European Court of Human Rights (ECtHR) held that blocking access to YouTube was illegal as there was no domestic law allowing for blanket orders blocking access to the internet.

Legitimate aim

The reasons for shutdowns, such as for slowing rumours, for ending cheating during examinations and for disrupting public protests, do not meet the limitation requirements of article 19 (3) of ICCPR. Legitimate aims should be construed narrowly, a criterion that is not met by the vague references made by African governments. Article 25 of the African Union Convention on Cyber Security and Personal Data Protection stipulates that

[i]n adopting measures in the area of cyber security and framework for implementation, state parties shall ensure that the measures adopted will not infringe in the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter, and other basic rights such as the freedom of expression.

Necessity and proportionality

The necessity of shutdowns cannot be proven as no transparent information exists as to the actual harm state officials intend to prevent and, where there is such, internet shutdowns have not been demonstrated to help mitigate these harms. The proportionality threshold is breached by the fact that shutdowns impact everyone within the targeted area, not only

those people engaging in a proscribed or prohibited activity. Proportionality does not only involve the number of people affected but also the severity and extent of infringement of the human rights of each individual. In *Ahmet Yildirim v Turkey* the ECtHR held that the judicial blocking of access to Google sites for hosting a website belonging to a person facing criminal proceedings was a violation of the right to freedom of expression since it blocked the access of other internet access and that less restrictive means could have been used.

Perhaps one of the most instructive legal expositions to create a causal link between the international law use of 'any other media' is the United States Supreme Court case of *ACLU v Reno*.³ In this case a formally-recognised connection was established between the internet as being a medium of expression, thereby qualifying as a form of media that can be subsumed under the international law jurisprudence of freedom of expression in the digital age.

Furthermore, Special Rapporteur Frank la Rue stated that the internet was a crucial method through which persons can exercise their right to freedom of opinion and expression.⁴ Most importantly, it may be argued that article 19 of the Universal Declaration at the time of its drafting had envisaged future changes in forms through which persons can assert their right to freedom of expression and opinion. This is one of the most prominent arguments for the internet to be regarded as one of such 'any other media' due to one of its key features being a medium of communication (Land 2008).

Article 9 of the African Charter provides for an unqualified right to access information and qualified right to freedom of expression and opinion as follows:

- (1) Every individual shall have the right to receive information.
- (2) Every individual shall have the right to express and disseminate his opinions within the law.

Under other regional human rights instruments, the right to freedom of expression is qualified just as it is under international law. However, the African Charter is the only instrument that does not qualify the right to freedom of expression, at least not explicitly or directly. As a buffer to the provisions of article 9 of the African Charter, the Declaration on the Principles of Freedom of Expression and Access to Information was adopted in Banjul in 2002. The Preamble to the Declaration emphasises the importance of respecting and promoting human rights through the use of ICT which includes the internet.

3.2.3 *The violation of freedom of association and peaceful assembly*

Association is a key component of any modern society. Political parties, private organisations and interest groups have become important aspects of social engineering through which socio-political socio-economic formations take place. These formations are an integral part of any

3 51 US 844.

4 Human Rights Council Resolution: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, A/HRC/26/30/Add.2.

democratic society due to the participation and involvement they generate in democratisation processes. The right to freedom of association and assembly, as a twin right used interchangeably, therefore solidifies the rights of citizens to join associations of their choice and also to organise for the general good of their interests, especially as established under ICCPR and the African Charter. The internet in its formation has become important in this regard. Hashtags are used politically to organise protests or create awareness on public policy concerns while people of common interests are encouraged to associate with people of like interests and views.

Due to the rallying characteristics of these two rights in the way in which they unify voices across the board and encourage diverse views on issues, the internet, being home to several of such diverse perspectives, was able to amplify and connect the public beyond physical boundaries. This organisation and association online, therefore, has led to several projections of violations of human rights and dwindling democratic fortunes in many countries in Africa. The affectation that connects the public has galvanised several movements beyond the reach of most African governments, in effect resulting in more political and economic changes in countries.

For example, during a nationwide protest in Uganda in 2016, the state ordered multiple shutdowns at different times in order to quell dissent during protests. Also, in Zimbabwe the government recently ordered an internet shutdown when citizens protested the hike in fuel prices in which many people lost their lives. Similarly, in Sudan the state ordered the cutting of communications networks in the country due to protests over the prolonged rule of Omar Al-Bashir, who eventually was toppled even in the absence of internet networks. This has also been the case in countries such as Cameroon, Egypt, Togo, Algeria, the DRC and many other countries. The right to peaceful assembly and association on the internet is one of the most potent rights that are infringed and violated by many autocratic states because of the power of new technologies to demand change in the most unified and persistent manner.

3.2.4 The violation of the right to political participation and access to public service

Shutdowns during elections and protests infringe on the right to direct political participation. In Gabon, the Republic of Congo, the DRC, Uganda and Chad, shutdowns resulted in less visibility for the opposition during or after the elections (Rydzak 2018). Additionally, the internet has offered new opportunities for governments to communicate with people (African Declaration on Internet Principles 2014). Seventy-one per cent of African political leaders and governments had a presence on Twitter as of June 2014 (Scott 2014). Political leaders and governmental institutions are increasingly using social media to pass on critical information that is essential for accessing public service. E-governance encompassing digitisation of the public service infrastructure has grown significantly in countries such as Kenya, Uganda and Nigeria as citizens access critical services and documents through online portals. Shutdowns, therefore, are likely to sever critical access to governmental platforms and services. During the shutdown in Zimbabwe, the government could not get critical information across to Zimbabweans. President Mnangagwa appealed for

calm on his Facebook and Twitter accounts, but the message could not reach Zimbabweans as the internet had been blocked (Aljazeera 2019).

Internet shutdowns sometimes are strategically executed to disenfranchise marginalised religious or ethno-linguistic minorities as a form of collective punishment. This occurred in Ethiopia where the Oromo ethnic group in Oromia was specifically targeted by internet slowdowns and shutdowns in March and August 2016 due to their long-term grievances against the government. In Cameroon, the internet shutdown was specifically extended in the country's Anglophone region where the President faced vocal opposition. Vulnerable groups such as migrants, refugees and women experience further intersectional barriers (Rydzak, 2018).

3.2.5 *The violation of the right to life, bodily integrity and security of the person*

Internet shutdowns are often used by governments to perpetrate impunity by causing gross human rights violations, violations of the laws of war and violence to be invisible to civil society, activists and the international community. Large shutdowns are often accompanied by paramilitary and military operations, making it difficult for documentation by citizen journalists and reporters, as happened in 2015 in Port-Gentil, Gabon and the Pool Region of the Republic of Congo in October 2015. In Sudan during the 2013 shutdown, dozens of protesters were killed during a crackdown after the shutdown had been enforced (Access Now 2016). Digital sieges often put vulnerable groups at risk of further violence from the military and militias and have led to the emergence of internet refugees, as people endanger their safety by undertaking hazardous journeys to areas with internet access, as happened in Anglophone Cameroon.

3.2.6 *The violation of the right to mental and physical health*

Internet shutdowns cause significant disruptions in the areas of emergency and healthcare services, resulting in the violation of the right to the 'highest attainable standard of physical and mental health' under article 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR). In 2017 a three-week disruption in Somalia hindered the delivery of critical medical paperwork involving crucial cases in addition to obstructing humanitarian assistance (Rydzak 2018). There have been reports of delays in life-saving procedures when medical specialists have been unable to contact one another as well as service breakdowns in hospitals that rely on digital technology. Disruptions would be particularly catastrophic if they were to coincide with a natural disaster.

3.2.7 *The violation of the right to education*

The right to education is a fundamental right as it enables effective participation of all in an open and democratic society, promotes tolerance and diversity, and furthers the maintenance of peace. The role of the internet in education has become increasingly significant as resources become digitised. Internet shutdowns to stem leaks and cheating during school examinations have undercut educational opportunities for all groups in the DRC, Ethiopia and Algeria. Internet disruptions impact

vulnerable populations disproportionately, particularly women and girls, especially in the area of Science, Technology, Engineering and Mathematics (STEM), as happened in Cameroon.

4 Democratisation and information and communications technology in Africa

As a precondition to good governance, human rights cannot be disregarded in analysing democracy in Africa. The role played by human rights in an African context reveals a positive change in most African governance systems. The introduction of international democratic standards to ensure and enhance political and civil rights has given a more holistic approach to democracy. In fact, human rights have offered a set of performance norms and different mechanisms to measure the integration and implementation of democratic principles such as accountability, transparency, impartiality and participation. As a result, in Africa most domestic and regional policies, such as the African Charter, have been drafted to protect and fulfil fundamental human rights. Hence, at the continental level there is also the African Charter on Democracy, Elections and Good Governance (African Democracy Charter) with its articles 2, 3, 4 and 5 which provide that state parties have the duty to ensure that the rule of law, human rights and democratic principles are protected and respected.

This new approach to democracy has globally assisted in monitoring inequalities at the continental level. As a consequence, human rights, especially civil and political rights, are more respected, and individuals are now empowered in many African countries. People are aware of their rights and benefit from an enabling legal framework to claim their human rights. Human rights have become an ultimate weapon for citizens with respect to government accountability, which enhances democracy.

The fundamental principles of human rights being designed to inform the legislative, judicial and executive frameworks, its implementation requires a stable and enabling context. However, in Africa, despite efforts made to harmonise domestic laws with international standards of human rights and democracy, the continent still encounters discrepancies between national and regional policies and the implementation system. Hence, designed to guide policies and programmes, in Africa human rights are yet to be incorporated in the system of governance because of the absence of strong enforceable measures.

As an example, elections, which are usually the first step towards democratisation, are often the period during which serious human rights violations occur. During the past decade, elections in Africa have generated several controversies regarding management and process (Adejumobi 2000). In fact, during the different stages from preparation, the actual elections to the post-electoral period, cases of serious violations of human rights have been recorded. Unfortunately, these common practices, such as election rigging, clientelism, unlawful constitutional amendments and last-minute delays or cancellations, reveal the weakness of African democracy (Adejumobi 2000). These irregularities often cause frustrations among populations. As a result, protests ensue offering

grounds for serious violations of human rights by the state through its so-called security agents.

Having a primary duty to respect, protect and fulfil rights, some African states have become perpetrators of violence or enhance its permissibility by the absence of sanctions in situations of violations of human rights. Therefore, although many states identify their respective countries as being democratic, it appears that in some countries only the concept has been added to the official name of the state without reflecting the country's political reality (Wiseman 1990). Due to the illegitimacy of electoral processes, the issue of the legitimacy of some governments in Africa often is questionable. The process of state building and democratisation requires the integration of the social, political and economic dimension of a specific country. However, as post-colonial states, African countries inherited their political systems from their previous colonisers and, therefore, they have missed the opportunity to build their own systems of democracy based on African values and standards of democracy.

For that reason, the AU takes democracy seriously by adopting the AU Constitutive Act 2000, 'to promote and protect human and peoples' rights, consolidate democratic institutions and culture, and to ensure good governance and the rule of law'.⁵ Therefore, since human rights are meant to empower people, African states have the responsibility to respect and protect human rights with sustainable strategies. especially in the age of new technologies that can represent both a threat to and an asset for democracy.

Articles 5, 6 and 7 of the African Democracy Charter deal with member states' responsibility to ensure adequate changes of government with transparency without failing to protect human rights. Additionally, article 8(1) goes further by insisting on the suppression of all forms of discrimination based on political opinion.⁶ In other words, the state is under the obligation to provide a democratic environment to its citizens where every individual has the liberty to choose and support a political party without fear of encountering discrimination or violence from the state or its agents.

The majority of these rights fall under civil and political rights that allow individuals to enjoy the inherent right to engage in public affairs by participating in the election of members of the government.⁷ These rights can only be exercised through a conducive political and electoral environment. With human rights activists raising the importance of holding free, fair and transparent elections with respect to the rule of law, technology becomes a strong tool and a means to protect human rights. In fact, it appears that with digital technology, exercising the rights cited above not necessarily requires the implication of the government.

In African countries, for instance, digital technology has enabled individuals to become aware of their fundamental rights and has created diverse channels to claim these rights through social media platforms. In addition, technology has been used in both advocacy and awareness-raising activities as well as fund-raising platforms to enhance human

5 Preamble of the African Union Consecutive Act.

6 Arts 5,6,7, 8(1) of the African Charter on Democracy, Elections and Good Governance.

7 UNHR Report, Monitoring Human Rights in a Context of Elections, ch 23.

rights. As far as transparency and accountability are concerned, technology has allowed people to monitor electoral processes in many African countries. Information concerning countries' budget allocations and international policies are also available and accessible to the public.

Technology has helped to build transnational movements and networks aimed at denouncing human rights violations at the international level. Technology, therefore, has removed boundaries and facilitated the realisation of the rights to freedom of expression, access to information and participation (Banisar 2010). At the continental level, during the past years, digital technology has contributed to enhancing peace, which has created a positive change regarding democracy, especially with respect to electoral processes. Digital technology has enabled the creation of advanced electoral monitoring systems, such as the biometric system, to ensure transparency and platforms the mapping of violence breakouts. This reveals governments' engagement and cautiousness in ensuring participation and accountability as a result of digital technology. In addition, digital technology has helped to reduce corruption with the adoption of electronic systems of public administration.

Therefore, it is important for Africa, moving forward with development, to design strategies to navigate in a context of digital technology by adopting a governance framework within which democracy and technology can coexist with the objective of protecting human rights (Banisar 2010). Developing strategies at both national and continental levels will enable Africa to be better prepared in dealing with the advantages and threats of digital technologies.

Therefore, despite the advancement in technological development, the stage of democracy in Africa is described to have deteriorated in the past years due to several violations of human rights in the digital age. The use of the human rights framework in the digital age to analyse democratic development in Africa reveals that many rights have been violated. For instance, 28 out of 54 countries have enacted legislation to address cybercrime, and a recurring feature of these laws is that they impede internet freedoms and human rights.⁸ This shows an adverse use of law and policy on digital technology in governance systems in Africa as a region.

Specifically, in some countries these laws are used as a legal basis for human rights abuses by states. In many instances, digital technologies have been used to repress people's rights to freedom of expression or to participate in public affairs. In countries such as Ghana, Liberia, Nigeria, Somalia, South Africa, South Sudan, Uganda and Zimbabwe, states have used measures such as an increase in the cost of data, internet shutdowns and surveillance, among others, to deprive citizens of the right to freedom of expression (MFWA, 2018). Additionally, regarding the rights to privacy, states have been using ICT as a means of collecting personal data for surveillance purposes to track down opponents. This often leads to the unwarranted arrest of civil society members or citizens based on

8 United Nations Conference on Trade and Development, *Cybercrime Legislation Worldwide* https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx (last visited 20 March 2019).

information shared on social media or communication networks (IGF 2018).

5 Combating internet shutdowns

When used effectively, an internet ‘kill-switch’ can paralyse a protest. It can leave activists unable to mobilise, and enable state agents to perform a wider range of human rights violations, comfortable in the knowledge that these overreaches will never make it to the wider global public. Given the far-reaching political and economic consequences of an internet blackout, there is an urgent need to recruit effective counter-activities to quell the issues posed by internet shutdowns. Some of these counter-activities are discussed below.

5.1 Judicial recourse

In order to make governments protect human rights in the digital age, national courts have become involved with internet shutdowns. For example, the High Court of Zimbabwe recently held that the Minister of State ‘did not have the power to switch off the internet’ (Swart & Mahere 2019). In Egypt, the Supreme Administrative Court imposed a fine of EGP 200 million on the President, on the Prime Minister EGP 300 million, and on the Interior Minister EGP 40 million for the 2011 internet shutdown, although these fines were later set aside (Sutherland, 2018). In Kenya, the High Court revoked a government order shutting down three television stations for broadcasting the inauguration of the opposition leader as the alternative President upon the latter disputing the process of conduct of the elections.

Traditionally, law and technology in Africa have interacted in a strange, recurring cycle. First there was the rapid development of impressive technologies that pushed the boundaries of cellular and internet communications. Then followed a series of belated legal reforms to regulate new industries and tame innovation. As innovation improves on the continent, respect for digital rights crawled behind at the lazy pace of the legislative process (Palmerini 2013). This cycle, however, is slowly being disrupted by efforts at strategic litigation, which has already secured key victories in several jurisdictions. By litigating important ‘test cases’ in national (and, later, supranational) judicial systems, activists for online freedom are able to effect long-lasting change ‘both inside and outside’ the courtroom (Open Society Justice Initiative, 2018).

A novel test on issues of network disruptions and human rights development came up in Zimbabwe in *Zimbabwe Lawyers for Human Rights (ZLHR) and Media Institute for Southern Africa Zimbabwe (MISA Zimbabwe) v Minister of State for National Security & Others* after local civil society took the government to court to declare an internet shutdown during

protests last year illegal.⁹ The High Court ruled against the government, setting aside an internet shutdown directed under Zimbabwe's Interception of Communications Act even though the decision was arrived at based on technicality. Despite justifications by the Minister for State Security, the Court decided for the petitioners, and ordered the state to 'unconditionally resume the provision of full and unrestricted internet services' – a major victory for internet freedom.¹⁰

A similar legal challenge gripped Uganda, after a targeted blackout had hit Kampala in May 2016 (Taye 2018). As voters took to the polls for the elections, they were hit by a 72-hour social media shutdown of sites including Twitter, Facebook and WhatsApp (Golooba-Mutebi 2011). Since the 2016 elections, the internet has become the newest feature of President Yoweri Museveni's efforts to silence growing opposition. In July 2018, the government introduced a 'social media tax' in a bid to increase domestic revenue and stop online 'gossip' (Al Dahir 2018). According to early reports, however, the tax is 'holding back' economic growth, shrinking profits, and placing thousands of jobs in jeopardy (Research ICT Africa 2018). To oppose the tax, and the recent spate of shutdowns in Uganda, Unwanted Witness – a local non-governmental organisation (NGO) – filed a petition before the Constitutional Court in December 2018 claiming, among others, a violation of article 29(1) of the 1995 Ugandan Constitution (BBC News 2018).¹¹ While the Court is yet to rule on the matter, this case highlights the emergence of new energies in the legal fight against internet shutdowns.

Similar legal proceedings have been instituted in Cameroon, Chad and Pakistan as internet freedom advocates cover more ground in the battle against shutdowns (Access Now 2018; BBC News 2018; *Telegeography* 2018;). Incremental as these efforts may seem, this gradual exhaustion of domestic remedies will unlock access to regional courts and other oversight mechanisms. If these tribunals rule that internet shutdowns are illegal, internet activists would make a significant step towards protecting internet freedom in Africa and elsewhere. While exploring the avenue of strategic litigation, digital rights advocates should involve the ICT sector in their strategies to combat internet shutdowns.

5.2 Mobilising the private sector

Resisting shutdown orders is potentially risky for internet service providers as they are bound by the laws governing their countries of operation, and non-compliance may result in licence revocations, fines, threats, or gateway shutdowns (Association for Progressive Communications 2019). Telco representatives have reported threats to employees on grounds of non-compliance with shutdown orders, as happened in Ethiopia (Ilori 2019). In Zimbabwe, the director of Econet wireless claimed that he had to comply with a shutdown directive from the

9 Case 265/19 (Provisional Order) 21 January 2019 (*Zimbabwe Shutdown Provisional Order*) <http://www.veritaszim.net/node/3396> (last visited 20 March 2019).

10 *Zimbabwe shutdown Provisional Order* (n 10) 2.

11 Which guarantees the rights to 'freedom of speech and expression which shall include freedom of the press and *other media*' (our emphasis). Sec 29(1) Constitution of the Republic of Uganda 1995.

government or face three years' imprisonment for non-compliance (Association for Progressive Communications 2019).

Over the past 50 years, Africa has leapt from the outdoor market to the online store, as internet access reoriented economic activities on the continent (Ernst & Young 2016). Tax benefits aside, the ICT sector makes a significant contribution to the micro- and macro-economies of African states, unlocking opportunities for inclusive growth and larger markets for local entrepreneurs (Bankole et al 2011). Abrupt disconnections are frustrating these opportunities, driving down profits and overall GDP (CIPESA 2018). Although a few studies suggest that strategies of political repression are implemented more effectively if the government controls the infrastructure, the role of telecommunication companies in enabling or disabling network disruptions has not yet been sufficiently explored (Weber 2011). To limit the impact of unlawful disconnection orders, companies should establish procedures (internally, for their boards of directors, and externally, for the ICT industry itself) to ensure accountability and enforce transparency in the event of an internet shutdown (Access Now 2016). By employing a combination of these strategies, the private sector can prove to be a powerful ally in the fight against internet shutdowns.

A failure to respond adequately to even a brief internet shutdown can have serious implications for a company's bottom line. In 2015 millions of Brazilians downloaded the mobile messaging application Telegram after a 24-hour court-ordered shutdown of WhatsApp (Griffin 2015). Those customers that defected are not returning to WhatsApp (Wong 2016). Profit motive aside, internet shutdowns carry with them reputational and other non-tangible costs that far exceed the financial implications of a temporary disconnection. Taking all these risks into consideration, companies have an obvious motivation for forming their own response to internet shutdowns. This response should be guided by the United Nations Guiding Principles on Business and Human Rights (UNGPs) which, despite well-deserved criticism, represent international consensus on the *minimum* obligations of companies to respect human rights (Okoloise 2017).¹²

According to the UN Guiding Principles, a company's responsibility to respect human rights applies in all situations and 'exists independently' of whether the state meets its own human rights obligations (UN Guiding Principles 2011). Furthermore, these responsibilities require companies to 'avoid infringing on the human rights of others' and 'address adverse human rights impacts' (UN Guiding Principle 2011). Citing this obligation as justification, 2016 saw telecommunications companies Millicom and Orange refuse government demands for internet shutdowns that were not made according to proper procedures under domestic law (Telecommunications Industry Dialogue 2016). In 2012 the Vodafone group and Orange, in response to shutdown orders in Egypt in 2011, established the Telecommunications Industry Dialogue (TID) to help

12 United Nations Human Rights Council 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie – Guiding Principles on Business and Human Rights: Implementation of the United Nations "Protect, Respect and Remedy" Framework' UN Doc A/HRC/17/31 (21 March 2011).

prevent future abuses (*Access Now* 2016). Since then, membership has swelled to include AT&T, Millicom, along with various members of international civil society.¹³ To focus its efforts, the TID established its own set of Guiding Principles (TID Guiding Principles) which address the corporate responsibility of telecommunications companies to respect human rights. Among others, the TID Guiding Principles require members to '[a]dopt, where feasible, strategies to anticipate, respond and minimise the potential impact on freedom of expression ... where a government demand or request is received that is unlawful' (TID Guiding Principles 2011).

More recently, ICT companies have encircled their weapons to better respond to demands of unlawful disconnection. Through the Global Network Initiative (GNI), companies such as Ericsson, Google and Nokia worked together with the TDI to issue a Joint Statement on Network and Service Shutdowns. The statement declares internet shutdowns to be a threat to public safety and freedom of expression, with the further danger of restricting access to vital payment and health services in the event of an emergency. In a similar vein, the Global System for Mobile Communications Association (GSMA), one of the world's largest technology associations, has laid out strict standards for orders issued to telecommunications companies to terminate service, relegating them to 'exceptional and pre-defined circumstances, and only if absolutely necessary and proportionate to achieve a specified and legitimate aim consistent with internationally recognised human rights and relevant laws' (GNI & TID 2016).

Companies in the ICT sector are catching on, and are beginning to realise that internet shutdowns are as bad for business as they are for human rights. While the outbreak of these new democratic pushbacks seems exciting, the private sector needs to implement broader reforms to comply with their obligations under international human rights law. Internet service providers and telecommunication operators should endeavour to uphold the rule of law by challenging illegal requests from governments (Glans & Markoff 2011).¹⁴ They should also be transparent with their customers around the sources of shutdown requests and communicate how long these disruptions are likely to occur. Further, when looking for opportunities to invest, venture capitalists should integrate shutdowns into their risk assessment to discourage investments in states that too hastily resort to internet shutdowns.

In many cases, an alliance with the private sector can be a formidable weapon in the hands of activists of digital freedoms. At the same time, however, human rights practitioners should be cautious in their engagement with telecommunications sector while noting that monopolies in the African telecommunications sector also pose threats to the rights to freedom of expression and privacy due to market dominance.

13 <http://www.telecomindustrydialogue.org/about/> (last visited 20 March 2019).

14 Vodafone, eg, resisted demands by Egyptian authorities for service interruptions until 'it was obliged to comply'; J Glanz & J Markoff 'Egypt leaders found "off" switch for internet' *The New York Times* 15 February 2011.

5.3 Multi-stakeholder approach

Several approaches are involved in engaging internet governance challenges. There have been the traditional and state regulatory means through which state authorities use laws and policies to determine the direction of internet governance. There has also been the private sector attempt at self-regulation, which looks to put private companies involved in internet governance as duty bearers in upholding human rights. However, all these models have failed mainly because of from where they emanate and how democratically the processes that inform their decisions are made (Garton Ash 2016). Since the internet is a collaborative system of networks, a policy initiative from one aspect of its stakeholder is bound to be mono-themed and unrepresentative.

This is one of the main motivations for the multi-stakeholder approach to internet governance, which looks to make the internet more open, people-focused and all-stakeholder-driven (Graham & MacLellan 2018). This approach registers the importance of the internet as technically democratic in design and functionally representative with respect to the policies that shape it. It allows for not only state and private businesses to come together to design approaches to internet governance challenges, but affords civil society, the academia and a broader spectrum of stakeholders to be involved in designing lasting policies for internet governance.

In resolving the challenges posed by internet shutdowns, a multi-stakeholder approach lends a good governance approach to assessing threats and managing risks associated with internet regulation. There are instances when restrictions of human rights through ICT could be justified, but such limitation must be narrowly construed, comply with international law standards and must be as a result of a multi-perspective deliberations.

6 Conclusion

It is undeniable that we are living in an era driven by clicks of the mouse and virtual interactions. Digital technologies have permeated our everyday lives – including the exercise, enjoyment and fulfilment of human rights. Human development across countries is tied to how much technology a society can adapt to its society to ensure improved living standards. While the study of ICT and the right to development is still growing, the maximisation of available ICT resources is currently on full throttle in many societies. However, the same cannot be said of other countries, especially in Africa. These challenges faced by many African countries include the violation of human rights; affordability of internet access; state-sponsored censorship; internet taxation; and network disruptions. These disruptions together with the other problems have hampered democratic development and pose huge threats to the right to development in the region. It is important, now more than before, for state and non-state actors to commit to a standardised set of rules, perhaps a model law on key thematic areas of digital rights in the region that involves all stakeholders including the courts, private businesses and civil society to engage the challenges of internet shutdowns in Africa.

References

- Access Now 'Pakistanis have long suffered from internet shutdowns. At last, their voices are being heard' 27 February 2018, available at <https://www.accessnow.org/pakistanis-long-suffered-internet-shutdowns-last-voices-heard/> (last visited 18 June 2019)
- Access Now 'Internet shutdowns: The risks and opportunities for technology sector investors' (2016)
- Access Now 'Primer on internet shutdowns and the law' (2016), available at https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/AccessPart_1.docx (last visited 15 March 2019)
- Access Now 'The state of internet shutdowns around the world' (2019), available at <https://www.accessnow.org/cms/assets/uploads/2019/06/KIO-Report-final.pdf> (last visited 19 June 2019)
- Access Now 'What is an internet shutdown?' (2019), available at <https://www.accessnow.org/keepiton/> (last visited 6 March 2019)
- Aljazeera 'Zimbabwe: Mnangagwa ends foreign tour early amid domestic turmoil' (2019), available at <https://www.aljazeera.com/news/2019/01/zimbabwe-mnangagwa-ends-foreign-tour-early-domestic-turmoil-190120171320583.html> (last visited 18 June 2019)
- Arts K & Tamo A 'The right to development in international law: New momentum thirty years down the line?' (2016) 63 *Netherlands International Law Review* 226
- Media Foundation for West Africa (MFWA) 'African government surged to prioritise digital rights' 11 January 2018, available at <https://ifex.org/african-governments-urged-to-prioritise-digital-rights/> (last visited 12 April 2019)
- 'Airtel, Tigo face hearing on bandwidth throttling' *TeleGeography* 13 September 2018, available at <https://www.telegeography.com/products/commsupdate/articles/2018/09/13/airtel-tigo-face-hearing-on-bandwidth-throttling/> (last visited 1 April 2019)
- Dahir AL 'Uganda's "regressive" social media tax may cost its economy hundreds of millions of dollars', available at <https://qz.com/africa/1375795/ugandas-regressive-social-media-tax-may-cost-its-economy-hundreds-of-millions-of-dollars/> (last visited 15 May 2019)
- Association for Progressive Communications 'Chad must end its year-long blackout of Social Media' (2019), available at <https://www.apc.org/en/pubs/chad-must-end-its-year-long-blackout-social-media> (last visited 24 March 2019)
- Association for Progressive Communications 'Internet shutdowns in Africa: "It is like being cut off from the world"' (2019), available at <https://www.apc.org/en/news/internet-shutdowns-africa-it-being-cut-world> (last visited 9 March 2019)
- Bankole FO, Shirazi F & Brown I 'Investigating the impacts of ICT investments on human rights' (2011) 48 *The Electronic Journal of Information Systems in Developing Countries* 3
- Bowman W & Camp L 'Protecting the internet from dictators: Technical and policy solutions to ensure online freedoms' (2013) 1 *The Public Sector Innovation Journal* 18
- Brown S & Kaiser P 'Democratisation in Africa: Attempts, hindrances and prospects' (2007) 28 *Third World Quarterly* 3

- 'Cameroon: NGOs sue government over internet shutdown for Anglophone region' *BBC News* 26 January 2018, available at <https://www.bbc.com/pidgin/tori-42828863> (last visited 19 May 2019)
- Cerf V 'Internet access is not a human right' *The New York Times* 4 January 2012
- Collaboration on International ICT Policy in East and Southern Africa (CIPESA) 'Despots and disruptions: Five dimensions of internet shutdowns in Africa' (2019) 9, available at https://cipesa.org/?wpfb_dl=283 (last visited 18 June 2019)
- Collaboration on International ICT Policy for East and Southern Africa (CIPESA) 'State of internet freedom in Zimbabwe 2016' (2016) 4 22, available at https://cipesa.org/?wpfb_dl=231 (last visited 15 March 2019)
- Collaboration on International ICT Policy in East and Southern Africa (CIPESA) 'A framework for calculating the economic impact of internet disruptions in sub-Saharan Africa' 11, available at https://cipesa.org/?wpfb_dl=252 (last visited 21 March 2019)
- Banisar D 'Linking ICTs, the rights to privacy, freedom of expression and access to information' (2010) 16 *East African Journal on Peace and Human Rights* 1
- Kibet E & Fombad CM 'Transformative constitutionalism and the adjudication of constitutional rights in Africa' (2017) 17 *African Human Rights Law Journal* 348
- Ernst & Young 'Global telecommunications study: Navigating the road to 2020' (2016) 10-12, available at [https://webforms.ey.com/Publication/vwLUAssets/ey-global-telecommunications-study-navigating-the-road-to-2020/\\$FILE/ey-global-telecommunications-study-navigating-the-road-to-2020.pdf](https://webforms.ey.com/Publication/vwLUAssets/ey-global-telecommunications-study-navigating-the-road-to-2020/$FILE/ey-global-telecommunications-study-navigating-the-road-to-2020.pdf) (last visited 21 March 2019)
- Freyburg T & Garbe L 'Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa' (2018) 12 *International Journal of Communication* 3896 3916
- Garton Ash T (2016) *Free speech: Ten principles for a connected world* New Haven & London: Yale University Press 250
- Glanz J & Markoff J 'Egypt leaders found "off" switch for internet' *The New York Times* 15 February 2011
- Graham B & MacLellan S 'Overview of the challenges posed by internet platforms: Who should address them and how' in E Donahoe & FO Hampson (eds) *Governance innovation for a connected world: Protecting free expression and civic engagement in the digital ecosystem* (2018) Waterloo: Centre for International Governance Innovation 11
- Global Network Initiative (GNI) & Telecommunications Industry Dialogue (TDI) 'Global Network Initiative and Telecommunications Industry Dialogue Joint Statement on Network and Service Shutdowns' (GNI &TDI Joint statement) 12 July 2016, available at <https://globalnetworkinitiative.org/gni-id-statement-network-shutdowns/> (last visited 12 May 2019)
- Golooba-Mutebi F 'As the Arabs rise up and conquer fear, black Africa looks on in gloomy envy' *The East African* 14 February 2011, available at <https://www.theeastafrican.co.ke/oped/434748-1106360-yshyaf/index.html> (last visited 12 June 2019)
- Griffin A 'Brazil's WhatsApp ban is driving millions of users to Telegram' *Independent* 17 December 2015, available at <https://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-brazil-whatsapp-chat-apps-ban-a6776941.html> (last visited 21 March 2019).
- Guerriero M 'The impact of internet connectivity on economic development in sub-Saharan Africa' *United Kingdom Economic Private Sector Report* (2015) 4, available at <http://www.telecomindustrydialogue.org/about/>; <https://african>

- internetrights.org/articles/; https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx; <https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/> (last visited 18 June 2019)
- Kaballo S 'Human rights and democratisation in Africa' (1995) 53 *Political Studies* 189
- Ilori T 'The impact of internet shutdowns in Africa' *AfricLAW* 21 February 2019, available at <https://africlaw.com/2019/02/21/the-impact-of-internet-shutdowns-in-africa/> (last visited 9 March 2019)
- Joyce D (2015) 'Internet Freedom and Human Rights' 26 *The European Journal of International Law* at 498
- Kazeem Y 'Having more rival mobile networks in a country often means cheaper internet for Africans' *Quartz Africa* 14 September 2018, available at <https://qz.com/africa/1390318/africa-has-the-most-expensive-internet-in-the-world/> (last visited 20 February 2019)
- Kiplagat S 'High Court orders state to restore signals for 3 TV stations' *Daily Nation* 1 February 2018, available at <https://www.nation.co.ke/news/Court-orders-State-restore-TV-signals/1056-4287466-ka8lie/index.html> (last visited 15 March 2019)
- Land M 'Toward an international law of the internet' (2013) 54 *Harvard International Law Journal* 394 458
- Maurushat A, Chawki M, Al-Alosi H & El Shazly Y 'The impact of social networks and mobile technologies on the revolutions in the Arab world: A study of Egypt and Tunisia' (2014) 3 *Laws* 682
- Morton S, Pencheon D & Squires S 'Sustainable Development Goals (SDGs), and their implementation' (2017) 124 *British Medical Bulletin* 82 83
- Mukeredzi T 'Uproar over internet shutdowns' *AfricaRenewal* (2019), available at <https://www.un.org/africarenewal/magazine/august-november-2017/uproar-over-internet-shutdowns> (last visited 13 March 2019)
- Nyabola N (2018) *Digital democracy, analogue politics: How the internet era is transforming politics in Kenya* London: Zed Books
- Okoloise C 'Contextualising the corporate human rights responsibility in Africa: A social expectation or legal obligation?' (2017) 2 *African Human Rights Yearbook* 191
- Open Society Justice Initiative (OSJI) *Strategic litigation impacts* (2018) 14
- Palmerini E 'The interplay between law and technology, or the RoboLaw project in context' in E Palmerini & E Stradella (eds) *Law and technology. The challenge of regulating technological development* (2013) Pisa: Pisa University Press 15-16
- Papacharissi Z (2014) *Affective publics: sentiments, technology and politics* Oxford: Oxford University Press
- Posner DN & Young DJ 'The institutionalisation of political power in Africa' (2007) 18 *Journal of Democracy* 127
- Paradigm Initiative 'Digital rights in Africa 2017 report' (2017) 2 61, available at http://www.intgovforum.org/multilingual/es/system/files/filedepot/78/paradigmhq-digital_rights_in_africa_report_2017.pdf (last visited 15 March 2019)
- Paradigm Initiative 'The 2019 Nigerian elections through the lens of digital rights' (2019), available at <https://paradigmhq.org/download/the-2019-nigerian-elections-through-the-lens-of-digital-rights/> (last visited 18 June 2019)
- Research ICT Solutions 'Unleash, not squeeze, Uganda's ICT sector' (2018), available at <https://researchictsolutions.com/home/unleash-not-squeeze-uganda-its-ict-sector/> (last visited 21 March 2019)

- Rydzak J 'Disconnected: A human rights-based approach to network disruptions' (2018) *Global Network Initiative* 4 27
- Selian AN (2002) 'ICTs in support of human rights, democracy and good governance' International Telecommunications Union, available at <https://www.itu.int/osg/spu/wsis-themes/humanrights/ICTs%20and%20HR.pdf> (last visited 17 June 2019)
- Said A 'Elections in Africa: A fading shading for democracy' (2000) 21 *International Political Science review* 59 73
- Scott G 'How should governments best use Twitter?' *Global Government Forum* 9 June 2014, available at <https://www.globalgovernmentforum.com/how-should-governments-best-use-twitter/> (last visited 14 March 2019)
- Sutherland E 'The internet and human rights: Access, censorship, shutdowns, and surveillance' (2018) *Institute for Advanced Legal Studies, University of London* 2 12
- Swart M & Mahere F 'Internet shutdowns violate human rights' *Mail & Guardian* 1 February 2019, available at <https://mg.co.za/article/2019-02-01-00-internet-shutdowns-violate-human-rights> (last visited 15 March 2019)
- Taye B 'Time is up: Uganda in court over internet shutdowns that violate human rights' *AccessNow* 8 November 2018, available at <https://www.accessnow.org/uganda-in-court-over-internet-shutdowns/> (last visited 15 May 2019)
- Telecommunications Industry Dialogue (TID) 'Submission on Freedom of Expression and the Telecommunications and Internet Access Sector' (2016) 9
- The Economist Intelligence Unit 'Democracy Index 2018: Me too? Political participation, protest and democracy' (2019) 2-51, available at https://www.prensa.com/politica/democracy-index_LPRFIL20190112_0001.pdf (last visited 15 March 2019)
- Villlaroman N 'Rescuing a troubled concept: An alternative view of the right to development' (2011) 29 *Netherlands Quarterly of Human Rights* 14
- West DM 'Internet shutdowns cost countries \$2,4 billion last year' (2016) *Center for Technological Innovation at Brookings, Washington DC*, available at <https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/> (last visited 15 April 2019)
- Wiseman JA (1990) *Democracy in black Africa. Survival and revival* New York: Paragon House
- Winkler IT & Williams C 'The Sustainable Development Goals and human rights review' (2017) 21 *The International Journal of Human Rights* 1023 1024
- Wong JI 'The messaging app that's benefiting from WhatsApp's ban in Brazil' *Quartz* 3 May 2016, available at <http://qz.com/675070/the-messaging-app-thats-benefiting-from-whatsapps-ban-in-brazil> (last visited 21 July 2019)
- 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 <http://www.achpr.org/press/2019/01/d440/> (last visited 15 March 2019)
- 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 Situation of Freedom of Expression and Access to Information in the Republic of Chad' 22 March 2019, available at <http://www.achpr.org/press/2019/03/d448/> (last visited 24 March 2019).
- General Assembly Resolution – A/HRC/28/L.10/Rev 1 (18 June-6 July 2018)

Human Rights Council Resolution 7/36; Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

Human Rights Council Resolution: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank la Rue, A/HRC/26/30/Add.2

Resolution on the Right of Freedom of Information and Expression on the Internet in Africa, ACHPR/Res. 362 (LIX)

UN Human Rights Council Resolution on 'the promotion, protection and enjoyment of human rights on the internet' (A/HRC/38/L.10/Rev.1)

United Nations Human Rights Council 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie – Guiding Principles on Business and Human Rights: Implementation of the United Nations "Protect, Respect and Remedy" Framework' UN Doc A/HRC/17/31 (21 March 2011)

Are smart walls smart solutions? The impact of technologically-charged borders on human rights in Europe

Bronagh Kieran, Fuensanta Amorós Cascales,**
Laura Thomi*** and Meredith Veit*****

Abstract: *This article reviews new technologies on the external border of the European Union, and the human rights ramifications of these developments. It utilises a multi-disciplinary approach, writing on the emerging technologies themselves, their impact on vulnerable groups, legal developments relating to privacy, and the political context informing migration policy. The first part outlines emerging trends in border technology. The discussion relies on examples beyond the European Union to inform its analysis, including case studies from the United States border with Mexico. Technological developments considered include thermal imaging; biometric data; virtual reality; artificial intelligence; and drones. The second part explores how vulnerable groups will be affected by the collection of biometrics at the external border of the European Union. This part explores how algorithms, far from being objective arbiters, in fact are repositories for the bias of the manufacturer. The article postulates that to tackle the proliferation of bias, it is necessary to have a diverse workforce creating these systems. Third, the article addresses the regulatory framework on data privacy in the European Union. The significance of a right to privacy post-9/11 context is described. The conception of data privacy of the General Data Protection Regulation (GDPR) is set out. This part first analyses how GDPR has affected the processing and storage of data in the EU and, second, draws out the implications for the data of migrants. Special emphasis is placed on the concept of consent, and the ability of migrants to refuse the collection of their data is put into question. Finally, the article turns to the political context. Arguing that right-wing populism is not inherently opposed to new technologies, the article points to populists' reliance on social media to garner support. Furthermore, it is advanced that the potential for migrants' human rights to be impinged by new technologies is compounded by the influence of right-wing populism on migration policy.*

Key words: *smart borders; surveillance; consent; privacy; biometrics; human rights; vulnerable groups; securitisation; technology; artificial intelligence*

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. BCL Law with Philosophy (University College Dublin) MA in Human Rights and Democratisation (Global Campus Europe).

** BA Law (Universidad de Alicante) MA in Human Rights and Democratisation (Global Campus Europe).

*** BSc in Social Work (Lucerne University of Applied Sciences and Arts) MA in Human Rights and Democratisation (Global Campus Europe).

**** BA in Communication and Public Culture (George Washington University) MA in Human Rights and Democratisation (Global Campus Europe).

1 Introduction

Since the end of World War II a significant number of border walls and fences have been erected around the world as a means of separating the in-group from the out-group. Metal, wire or concrete walls separate Greece from Turkey, Turkey from Syria, Spain from Morocco, Morocco from the Western Sahara, Hungary from Serbia, Israel from Egypt, Israel from the West Bank, Saudi Arabia from Iraq, Iraq from Iran, Malaysia from Thailand, Zimbabwe from Botswana, the United States from Mexico, Pakistan from India, India from Bangladesh, North Korea from South Korea, and the list continues. The European Union (EU) has over 1 000 kilometres of fences or walls guarding member states against non-member states, according to a recent study by the Transnational Institute (Ruiz Benedicto & Brunet 2018). In the 1990s the EU had two walls, while in 2019 there are now 15 walls (Ruiz Benedicto & Brunet 2018).

Since the 9/11 attacks in 2001, the construction of these physical barriers has spiked even further, as leaders preach the imperative urgency – even as a national emergency – of keeping migrants out and nationalists in, furthering a xenophobic ‘us versus them’ mentality. Governments seemingly build these walls with the unrealistic expectation that they will render their citizens impervious to the effects of any hardship beyond their barbed wire limits. However, as the opposition argues, they are a medieval solution to a twenty-first century problem. As we shift from emergency-driven policies to intelligence and risk management policies, many populist leaders currently in power are offering walls as the simple solution to complex immigration challenges. With this shift to risk management policies, which focus on prevention to obtain the maximum security, proportionality tests should be carefully made since civil rights and liberties could be at stake.

Populist rhetoric revolves around state identity and the consolidation of state sovereignty. This is often tied to an anti-immigrant agenda, whereby immigration is blamed for citizens losing control of their country. In this sense, border walls are emblematic of the populist conception of sovereignty. The militarisation of borders and border walls also feeds into an extremist narrative of state sovereignty, as it implicitly reinforces the divisive rhetoric which portrays immigrants as ‘invaders’.

Offered as an alternative and more rational solution, many politicians of the developed world propose intensifying the role that technology plays in determining who can cross over from one state into the next. This article explores the advantages and disadvantages of building digital walls. It examines possible human rights benefits of border technologies, but argues strongly in favour of necessary precautions for integrating innovations from the Fourth Industrial Revolution¹ into states’ immigration processes and systems. As technology evolves, it seems that the watchful eye of governments can be overreaching: collecting data without consent, peering over state lines, and treating civilians as suspects.

1 According to Prof Klaus Schwab (2016), founder and executive Chairperson of the World Economic Forum, the fourth industrial revolution involves imbedding technology into people’s everyday lives, and even into their bodies, made possible by advancements in biotechnology, the Internet of Things (IoT), artificial intelligence, robotics, nanotechnology, quantum computing, and more.

But the application of technological advancements can reap true benefits if implemented with a human rights framework in mind. State sovereignty is also affected by technologically-established frontiers in so far as they grant the state additional access to – and, potentially, control over – personal data. This article explores the most advanced technologies being used at the border and plans for future technological integration at transit checkpoints. In analysing topical case studies, the current legal framework and the overall political environment, we aim to critically review how travellers' human rights are being (and potentially could be) impacted.

Moreover, while these technologies redefine the concept of border, they also reaffirm it. Tangibly crossing the border can now involve more than just treading over a single 'line in the sand' and passing through an immigration checkpoint. Now, the areas surrounding the border also include surveillance technologies associated with border control and potentially cause even further human rights violations, particularly considering the effects on vulnerable groups. This is linked to the so-called militarisation of borders. In this way, even where physical walls are not built, strong barriers 'protecting' the state from immigrants may nonetheless be constructed from 'smarter' materials. Security concerns are regularly conflated with questions surrounding immigration policy and the technology it hires. However, this creates a false dichotomy between human rights for immigrants and national security.

The tendency to move towards a 'surveillance society' has also produced a significant shift in citizens' perceptions of both personal privacy and security. As populist discourses in Western societies foster a 'culture of fear' and 'overprotection', so too does the notion that in order to have security, one must relinquish one's privacy. Within this privacy-for-security trade-off, infringements upon privacy and other human rights arise, and along with them questions about the compatibility of constant border surveillance with democratic societies.

Indeed, a pressing problem is political rhetoric that positions migrants as a serious risk to national security, regardless of a connection with arms or human trafficking, drug smuggling, or terrorist activity. This inherently threatens the idea of maintaining human dignity, even more so at the hands of intelligent machine intervention. Security concerns are being paired with a strike against 'illegal' migration,² as wars in the Middle East and gripping economic distress and violence in Central America have forced migrants from their dangerous and impoverished nations towards the Western world. In 2015 and 2016 Frontex, the European Border and Coast Guard Agency (nd) detected more than 2.3 million 'illegal crossings'. Refugees are widely considered to be the new 'threat' and anti-immigrant rhetoric is fuelling the desire for states to close their borders, which will be further discussed in part 6 of this article.

Furthermore, the use of more advanced technology attempts to reconcile two aims of the state that are often contradictory, namely, 'facilitating the movement of people while increasing the level of control

2 Based on legal terminology, 'illegal' immigration occurs when a person crosses into a state's territory without permission from the government. For the purposes of this article, we will refer to mass migration movements as irregular migration so as to not further stigmatise the affected groups.

over them' (Kosłowski 2011). This causes tensions between the freedom of movement as well as rights to privacy and security. Security-privacy tradeoffs and the effects of border digitisation on data security and privacy protection will be examined in part 5 of this article.

Finally, scholars have long declared the necessity of integrating ethics and human rights considerations into the development and use of advancing technologies (Bowling, Marks & Murphy 2008: 41). Part 4 of this article argues that greater attention should be given to how furthering the capacities of 'virtual fences' and 'smart borders' impacts all people, regardless of nationality or side of the border, particularly those considered most vulnerable. First, however, the next part sketches the historical development of border technologies, before part 3 provides an overview of state of the art of digital borders.

2 Background and historical development of border technology

Physical borders have traditionally 'marked the limits of sovereign territory and acted as the primary site of expression of the exclusionary powers of the state' (Pickering & Weber 2006: 19) determining who and what should be allowed to cross onto domestic soil. Yet while globalisation intensifies, so does the flow of people, goods and conveyances across geographic lines, making maintaining territorial sovereignty an ever-daunting challenge for border-control authorities (Kosłowski 2011). Over the past three decades, substantial increases in funding, staff and technological capabilities used towards surveilling states' air, land and maritime frontiers have amplified political contention over the most efficient and effective ways to maintain a national stronghold (Kosłowski 2011). While many specialists argue for a multi-pronged approach to security (Meyers 2003; Mittelstadt et al 2011) deploying more advanced technology – more specifically in the form of algorithmic additions, Internet of Things (IoT)-based information systems and biometrics – is widely considered the 'magic bullet' solution to filling the problematic gaps left by solely erecting physical barriers (Ceyhan 2008: 19; Marx 2005: 9).

As technology evolves, so does its varied applications. However, states that are employing these new technologies for border control purposes cannot be absolved from their responsibility for the resultant human rights implications, regardless of geographically-imposed boundaries. Katja Franko Aas (2005: 22) argues that 'contemporary technological paraphernalia ... not only enables fortification of the border, it also reshapes the border according to its own logic', meaning that a concrete definition of a border can no longer be accurately drawn on any map. The expansive reach of technological capabilities can extend miles beyond any previous understanding of nation-bound jurisdiction.

2.1 The evolution of technology at international transit-points

From the 1970s until the present, states have been using surveillance technology in order to 'make visible the invisible' in terms of politically-determined threats (Haggerty & Ericson 2000: 620). Initially, states installed portable electronic intrusion-detection ground sensors and low-light video cameras at their borders in order to better monitor migrants

and traffickers on the ground (Koslowski 2011). However, the equipment lacked effectiveness as it was difficult to determine whether the person or thing that triggered the sensors actually was a threat. Additionally, the video quality on the low-light cameras was extremely poor. At airports, an identity document typically was not required for air travel. Airlines, being generally opposed to conducting individual screenings according to company policies, merely requested suspicious passengers to pass through a metal detector (Gardiner 2013). In the 1990s all metal items were subject to screening through an X-ray machine in search of weapons, and passengers' checked bags were usually only screened on international flights (Gardiner 2013). At this time, certain state borders were more equipped with motion, infrared, seismic and magnetic sensors in order to collect a clearer image of who or what was approaching state lines. By 2000 the United States government had placed approximately 13 000 ground sensors along the US-Mexico border (Gardiner 2013). As camera quality improved, the addition of images and sensors made it possible to determine how many people were on the other side of the border, where they were moving and in which direction, as well as whether or not they were carrying weapons.

Since 9/11 the US has led the global trend of thickening borders, making them less porous and more deflative. Following the attacks, the Transportation Security Administration (TSA) was created in 2001 and the US Department of Homeland Security (DHS) was created in 2003; the DHS quickly began 'including increased manned aerial assets, expanded use of unmanned aerial vehicles (UAVs) and next-generation detection technology' (2005) on US borders. TSA soon commissioned new full-body scanners within all international airports (Arnold 2010). A globally-piercing societal fear which revolves around an imagined 'low probability, high consequence' event is just one consequence of terrorism (Amoore 2013: 11), and national borders and immigration checkpoints have become physical spaces where citizens can tangibly understand the management of catastrophic risks.

Governments introduced data-collection mandates and heightened security screenings in order to create databases of biographic, immigration, and criminal histories of individuals, which are now 'shared among law enforcement agencies in a fashion unprecedented before the 2001 terrorist attacks' (Chishti & Bergeron 2011). The US signed bilateral Smart Border Declarations with Canada and Mexico in December 2001 and March 2002, respectively, calling for the standardisation of biometric data processing for all types of travellers – tourists, migrants and refugees included (Meyers 2005: 14). Immigration policy around the world is now based on information sharing between intelligence agencies as well as international, state and local law enforcement, all of which are increasingly reliant on the latest technologies to collect this data (Mittelstadt et al 2011: 5-9).

Countries around the globe have invested billions of taxpayer dollars into information technology-based programmes such as the Secure Border

Initiative (SBI);³ the Electronic System for Travel Authorisation (ESTA); automated biometric entry-exit systems such as US-VISIT and Europe's EES; registered traveller systems such as NEXUS, Global Entry and SENTRI; Electronic Travel Information and Authorisation Systems (ETIAS); the Schengen Information System (SIS II); and more (US CBP nd). Government budgets for border control are ballooning under the justification of mitigating alleged national security breaches. The EU announced its €34,9 billion spending plan for 2021 to 2027 on border infrastructure including scanners, automated licence plate recognition systems, and mobile laboratories, as compared to €13 billion from the previous period (European Commission 2018b). Meanwhile, the European Commission (2018a) announced their support towards EU agencies managing security, border and migration management, valued at €14 billion, in comparison to the €4,2 billion from the previous session. The US has spent approximately \$41 billion for border security since 2001 (American Immigration Council 2017) and President Trump's proposed wall would cost upwards of \$5,7 billion to complete (Nowrasteh 2019). According to Jean-Claude Juncker, President of the European Commission, '[b]etween now and 2027 we want to produce an additional 10 000 border guards. We are now going to bring that forward to 2020' (Angelescu & Trauner 2018). The US Immigration and Customs Enforcement (ICE) has more than doubled in size since President Trump took office (Politifact at the Poynter Institute 2017) and now employs more than 20 000 law enforcement and support personnel.

In 2016 the United Kingdom and France concluded a deal to construct a £2,3 million wall preventing refugees from entering French ports and boarding transport vehicles bound for the UK. The project requires an additional £44,5 million for additional fencing, closed-circuit television (CCTV) surveillance and other detection technology (Travis & Stewart 2018). In India, the Minister of State for Home Affairs, Kiren Rijiju, announced in 2018 that 'a pilot project for deployment of Comprehensive Integrated Border Management Solution (CIBMS) which includes different types of sensors, radars, day and night vision cameras, etc, has been taken up' to prevent the 'infiltration' of foreign threats into Indian territory (The Economic Times 2018). Brazil, too, announced in 2013 its plans to construct a \$13 billion virtual wall that will stretch 10 000 miles across 10 border countries, citing the need to curb illicit activities (Moura & Garcia-Navarro 2013). According to predictions by the market research company Frost and Sullivan, the global border protection and biometrics market is projected to grow from \$16,5 billion in 2012 to \$32,5 billion by 2021 (Ring 2013). Border security and immigration enforcement funding has an ever-increasing budget which is, at least partially, spent on cutting-edge equipment, as further explored in the next part (US ICE 2018; EOP 2019).

3 In 2006, the United States government commissioned Boeing to create a 'virtual wall' along the southern border, but the project was completely terminated in 2011 after being deemed a failure by the Government Accountability Office: '[a]bout 1,300 SBInet defects had been found from March 2008 through July 2009, with the number of new defects identified during this time generally increasing faster than the number being fixed — a trend that is not indicative of a system that is maturing and ready for deployment.' Around \$1 billion had been spent on the project by the time it was cancelled (U.S. GAO, 2010).

3 Constructing digital walls and data-driven barriers

Technology is neither inherently good nor bad, and its simultaneous ability to both cause problems and solve them is what provokes antithetical feelings of awe and apprehension. Arguing for whether or not technological advancements bring about more harm than good is rooted in the effects of their applications, but the full extent to which governments are implementing new technologies for securitisation remains unknown. Behind the semblance of national security, certain research and development initiatives as well as the scope of civilians' data utilisation are kept secret. What the public understands is based on the information they are allowed to know via government press releases, company reports from technology suppliers and developers, investigative reporting, and eyewitness or experiential testimony. The full picture is incomplete, but the evidence that has been disclosed thus far is unfavourable from a human rights perspective.

However, this is not to say that the technologies described in this part are not useful for protecting civilians from legitimate threats, such as violent actors or destructive weaponry, and the aim is to vilify neither border patrol nor the military. To date, it would seem that border technologies are not being applied with a human rights-bound mission in mind. Technology that has otherwise been used in wartime now is targetedly aimed at migrants, and the consequences of unquestioned civilian surveillance are already apparent along EU and US borders.

3.1 Technologies currently in use at the border

While steel fences and concrete walls lined with barbed wire continue to be erected around the world, military contractors are leading the armament of traditional border barriers with high-tech surveillance features and aerial reconnaissance (Vallet 2016: 53). Advancements in surveillance were the first upgrades for border patrol stations, as global increases in cross-border traffic corresponded with augmented pressure for states to monitor and manage this movement (Broeders 2011: 21). Primarily involved in the development of aerospace and defence technologies, companies such as Raytheon, Northrop Grumman, Lockheed Martin, Boeing and Ericsson now are repositioning their products towards protecting national frontiers against more abstruse threats – as opposed to identifiable enemy combatants. Aside from the major players, there are also many new market entrants attempting to capitalise on the global multi-billion dollar border security market, a few of which have already begun testing their products for further iteration. Since the US continually spends more on border control than any other country, most implementation trials take place along their borders, as discussed below.

Radars transmit radio waves in order to determine an object's position and velocity, while various types of sensors may use light or heat to detect objects. In the town of Roma, Texas along the US-Mexico border, patrol agents use Tethered Aerostat Radar System (TARS) blimps⁴ watch towers, drones and helicopters with powerful infrared sensors that were

4 Which are similar to Joint Land Attack Cruise Missile Defence Elevated Netted Sensor System (JLENS) blimps, which are an armed version of the blimp (Raytheon nd).

repurposed from the Department of Defence's missions in Afghanistan (Long & Barrios nd); this machinery was previously used to track and monitor the Taliban (Nixon 2017). TARS use two tethered, helium-filled airships, called aerostats, that float around 10 000 feet (around 3 000 meters) in the air. The blimp can be as large as the length of a football field, and can scan a territory the size of Texas (Raytheon nd), clearly extending far beyond the immediate radius of the borderline itself. While the blimps have been successful in detecting impending aircraft attempting to airdrop drugs across the border, they are also capable of detecting vehicles and other moving objects for miles within Mexican territory. This brings into question the legality of whether or not the US should be able to peer over into the lives of foreign citizens, placing an unconsensual hovering eye over communities that may not even be alongside the border.

Quanergy, a Silicon Valley startup, is testing the installation of its LiDAR sensors along the US-Mexico border. LiDAR stands for Light Detection and Ranging, which is a remote sensing method that pulsates light to measure distance and graph shape, and it is the same laser-based processing that gives operable vision to self-driving cars (National Ocean Service 2018). The laser can detect objects and humans in a variety of weather conditions, during the day or night, providing real-time three-dimensional object classification and tracking (Quanergy Systems 2018). LiDAR can use 'topographic, near-infrared lasers' to map the land, and 'bathymetric water-penetrating green lasers' to measure seafloor and riverbed elevation levels (Quanergy Systems nd). These sensors allow for machines to 'see' their environment, even below water. This could be used in search and rescue missions to save the lives of refugees who have fallen overboard, but instead it is being used to facilitate their capture.

Radars with 360 degree surveillance, light, heat and soundwave sensors are built into military-grade drones, drive-through beams, and individual body scanners. Thermal fencing is also a solution offered by many defence companies, using heat-detection as a means of monitoring perimeters. As described by Josef Gaspar, Chief Financial Officer of Elbit, an Israeli defence contractor, '[t]he electronic solution has far more advantages than any physical [barrier]. It detects early, long range, and the information is gathered from multiple sensors' (Reed 2016). The problem arises when these radars and sensors are being used to locate and track migrants, which leads to overcrowded detention facilities.

While sensors collect data concerning object location and classification, other thermal imaging and high resolution cameras are conjunctively operating in order to further detect and identify moving people on the ground. Unmanned aerial vehicles (UAVs or drones) combine cameras, lasers and sensors, and although they are increasingly used they are relatively cost-inefficient. US Customs and Border Protection completed 635 drone missions in the 2017 fiscal year, totaling over 5 625 hours of flight (Office of Inspector General 2018). The US flies nine drones along the southern border, but they have only assisted in 0,5 per cent of apprehensions at a cost of \$32 000 per arrest (Bier & Feeney 2018). This cost does not account for the value of privacy, which is fully neglected since no warrants are needed for border patrol-related UAV use. However, as argued by Koslowski and Schulzke (2018), drone surveillance also creates new accountability mechanisms, and supervision of patrol officers

may also lead to more calculated and cautious behaviour by police and guards.

Elbit,⁵ an Israeli defence contractor, has created a Groundeye system that can establish 'virtual safe zones' which establish an invisible fence around the perimeter of an area via mast-mounted tripods that notify operators when a person or vehicle crosses into the 'safe zone' area. Groundeye is able to 'zoom into multiple target areas of interest, while offering easy maneuverability between different areas according to operational requirements, and facilitating continuous reception of data and video coverage as well as high-quality image resolution in all areas of surveillance', which applies to both sides of the border (Elbit Systems 2016). Similarly, Northrop Grumman positions itself within the border patrol market by selling intelligent AlertVideo surveillance and geospatial imaging systems, which the US Marine Corps have used to improve decision-making capabilities for military operations along coastal zones (Fleming et al 2009: 213). The company describes these systems as being able to 'extract valuable behaviour and event information from existing surveillance systems and provides instantaneous visual and audible alerts' to the border patrol officers on watch (Northrop Grumman 2004). These integrated IoT communications networks are more quickly collecting information from previously-installed technologies, categorising that data and sending it back to government agencies. If migrants are considered to be a threat, then determining what is 'valuable' information to extract from surveillance footage can be interpreted varyingly, and whatever information is collected is systematically done without prior consent of the individuals.

Graduates of MIT's Media Laboratory founded Zebra Imaging in 1996, which first sold its holographic printers to the US military for deployment strategising in Iraq. However, now three of these million dollar printing machines are stationed at border crossing points in San Diego, Tucson and El Paso. To create these holographic maps, a drone first captures an aerial photograph of the border zone, and then uses the 360 degree view that the machine creates to construct a three-dimensional display of the landscape on the ground, better allowing for realistic targeting when deploying missions. Rick Black, director of government relations for the company, stated that 'the government brings in multiple agencies in emergencies that may not all operate in an area – like with the large Central American migrant issue', referring to the flow of migrants from Guatemala, Honduras and El Salvador that have been travelling north into Mexico and the United States (Hoffman 2016). 'Now [border patrol] can all understand where they are', Black explained, 'There's nothing else out there like this printer in the world' (Hoffman 2016). The EU Travel Information and Authorisation System (2017) credits holographic visualisation as an important tool for its security operations: 'The images

5 Elbit Systems is also a prominent company in the military defense technologies and services, with a presence in Europe, the Americas and Asia. Elbit describes itself as a company that sells 'digital soldiers' for a nation's combat needs, and has been granted multi-million dollar contracts to secure national borders. Elbit was responsible for building the 'smart' wall along the entirety of Israel's border with Egypt, which is both above and below ground. The wall was completed in 2013, and while there were around 12,00 migrants crossing this border in 2010, only about 12 crossed in 2016 (Elbit Systems, n. d. b; Elbit Systems, n. d. a; Reed, 2016).

create better battle-space awareness in order to give border security a better vantage point when trying to prevent or defend themselves against danger. Should danger actually strike, the holographs can be used to evacuate areas and help in recovery efforts.' In this instance, the discourse seemingly is directed towards combating terrorist activity along EU borders, but it is not specified. Rather than using this technology to intercept migration flows and capture refugees, states could better protect migrants in the event of extreme danger. Refugee camps are typically overcrowded with confined streets and layered cohabitation, and 3D models of the sites could help to better plan and execute emergency evacuation plans in the event of terrorist activity or a natural disaster. There is no evidence that this technology is being used to protect all lives, only American and European lives.

Member states of the EU and the regional body itself have for over a decade been logging, storing and monitoring migration databases concerning the inflow and outflow of passengers (Broeders 2007: 71). All the information collected is then analysed through centralised intelligence stations, where the data must be processed, stored and disseminated in a useful way. With such amassed amounts of data, algorithms are being used to analyse the content more quickly – an example being IDEMIA's Morpho Video Investigator, which automatically hones in on faces, bodies, motion and licence plates (IDEMIA nd). Algorithms are simultaneously sorting through video footage while also referencing volumes of raw data in order to record and classify elements deemed to be 'of interest' to law enforcement and the intelligence community. The greatest risk lies in misappropriated uses of what the government deems to be 'of interest'. The EU Travel Information and Authorisation System (2017) determines that any border technology implementation will work towards fulfilling the 'same goal of keeping citizens as safe as possible from terrorism and illegal entry,' thereby posing refugees as a threat and equating a person fleeing conflict with a terrorist. IDEMIA (nd) is already in use by governments within Europe, Latin America, the US, Asia and the Pacific, but not all countries have policies stipulating how the algorithmic conclusions of the system can be ethically used. There have already been instances when government-collected data is kept longer than presumed legal, which was the case when 35 000 images of citizens' body scans from TSA airport security leaked in 2010, even though US policy stated that all images are 'automatically deleted from the system after it is cleared by the remotely located security officer' (Johnson 2010). Global inconsistencies in how these algorithms are translated into government policy and an overall misunderstanding of how said policy is implemented leave ample room for mistakes without consequence.

3.2 Technology of the future, happening now

Collecting biometric data, via fingerprinting, has been a means of border-crossing identification for travellers since the mid-1990s when the United States created IDENT, the Automated Biometric Identification System (Gemalto nd). Worldwide, it has become more commonplace that fingerprints are taken at international transit points, and this personally identifying stamp can be used to determine an individual's eligibility for entering or exiting a country. Biometric data, as defined by the European Commission's Department of Migration and Home Affairs, is 'data relating to the physical, physiological or behavioural characteristics of an

individual which allow their unique identification, such as facial images or dactyloscopic data' (European Commission nd). Biometric data collection has since evolved to include the reading of irises, facial bone structure, the distance between one's eyes, nose and mouth, and so forth. The IT systems incorporated into the machinery that have been mentioned thus far in this report often store biometric data. All individuals participating in the US-VISIT programme – including persons with visas and green cards – must submit digital photographs and fingerprints providing biometric data to the federal, state and local governments (Mason nd). To date, biometric data and other personal information has been collected from over 200 million people who have entered, attempted to enter, or exited the United States (Gemalto nd). While the US plans to install more advanced biometric-based systems in all major airports within four years (TSA 2018), biometric data is also a required component of applications to enter Schengen states, which have collectively issued 14,6 million visas for short stays in 2017 alone (Schengen Visa Info 2018). On 8 April 2019 Singapore's Immigration and Checkpoints Authority (ICA) (2019) began testing iris scanning as a means of identification that replaces the need to show a passport. The iris scanner logs the unique patterns within the coloured circle of the eye, and capturing a person's biometric stamp only requires a person to look at the camera for one to seven seconds (ICA 2019). ICA states that the government's back-end database will determine if the traveller holds a valid passport and necessary visa in order to grant access. While iris recognition improves identification accuracy, reduces the likelihood of forgery and enhances efficiency at transit points, the tech companies that are incorrectly describing this technology as 'non-invasive' considering data could be collected surreptitiously, without individuals' knowledge (EFF nd). Additionally, if this information is hacked or leaked, then the responsibility lies with the third party vendor where the databases are stored and citizens may not even know that their information is being housed within these companies. If the result of non-compliance is the denial of access to the country, then ultimately the traveller is left with no choice as to whether or not they consent to have their irises read.

Anduril's Virtual Reality (VR) devices, backed by artificial intelligence, are currently undergoing testing by US Customs and Border Protection along the Texas border (Levy 2018). These devices, however, are not simulation based; they are being fed live information that is picked up by radars and laser-enhanced cameras that have been installed at high altitudes for a grander purview. The surveillance equipment can detect motion at approximately a three kilometre radius, and then locks on a target to determine its classification – 88 per cent likelihood of it being a person; 93 per cent likelihood of it being a plant; 76 per cent likelihood of it being an animal, for example (Anduril nd). The software that allows for communication between these systems is called Lattice, which synthesises data from potentially thousands of sensors and translates that into images on a Samsung Gear VR headset. On screen, the categorisations are highlighted making it easier for the human eye to determine where a target is moving or if an object in motion is worth noticing. Although still undergoing tests for further development, Lattice's experimental trial in Texas already assisted customs agents in detaining 55 'unauthorised border crossers' (Wodinsky 2018). According to their current business model, the data Lattice collects will belong to whatever agency has purchased a leased contract for the technology.

Based on the direction and rapid frequency of technological updates, it is likely that facial recognition technology will start specifying classifications of people that are seen through the VR goggles – by sex, gender, age, nationality, criminal status, and whatever other information the government may wish to reference against volumes of big data. China, for example, a country known for hyper-surveillance, has been using facial recognition technology to track and control the Uighurs (Uyghurs), a Muslim minority group. This has been called the first known example of a government utilising artificial intelligence for racial profiling, leading towards a ‘new era of automated racism’ (Mozur 2019). With this kind of virtual reality software serving as a gatekeeper for our borders, the potential for ethnically-motivated segregation is a grave concern.

Artificial intelligence is the science of building technology that can mimic human intelligence by instilling ‘logic’ into an algorithm or machine. Machine learning is a subset of artificial intelligence, and is based on a machine’s ability to make choices based on algorithms that feed neural networks and decision-making models, which are continually adapting to new information in order to self-improve. The ability for a machine to change algorithms as it learns more information is what differentiates machine learning from the broader category of artificial intelligence, and both of these advancements are being quickly adopted by law enforcement. In 2017 the West Midlands Police Department in the UK announced the development of a system called NAS (National Analytics Solution), which is a predictive model that can ‘guess’ the likelihood of someone committing a crime (Portilho 2019). The programme utilises machine learning as a means of combining related data sets – from other partner agencies as well as the Department of Education, the Department for Communities and Local Government, the Department for Work and Pensions and the National Health Service – to determine statistical probabilities prior to a person having committed the offence (West Midlands Police nd: 22). Therefore, neural networks will process data sets regarding people’s employment status, education levels, community involvement and health conditions (potentially mental and physical) in order to predict whether or not they are a threat to society. This kind of preemptive judgment has massive human rights ramifications, targeting individuals prior to an actual offence having been committed – nullifying the entire conceptual understanding of a right to a fair trial. The Alan Turing Institute’s Data Ethics Group (2017: 5) denounced the use of NAS, stating that ‘[w]e are generally concerned that the development of ethical principles in the NAS is not at a sufficiently advanced stage to permit them to keep abreast of the proposed uses of technology and data analytics for a new and wider law enforcement mission’. Border patrol is considered a branch within law enforcement, although thus far there is no evidence of patrol agents utilising this technology.

While machine learning is becoming pivotal in the field of medicine for more accurately diagnosing disease, and businesses are becoming more heavily reliant on its ability to sort through large amounts of data and detect patterns, a major underlying flaw in using machine learning for profiling is that the datasets may be biased or even doctored (Papernot et al 2017: 13). It is possible to reverse engineer algorithms in order to produce a desired output, which is why the true intelligence of the machine is influenced by the prejudice or intentions of its creator. Regardless, the artificially intelligent machines at our borders lack the

contextual knowledge of what human rights are, and have yet to be programmed with valuable insights on important bigger picture factors, such as the causes of global migration waves, personal concerns of privacy infringement, the stark effects machine decisions can have on an individual's life, to name just a few.

While humans are trying to teach artificial intelligence to machines, researchers are trying to recreate the marvels of nature by studying the flight patterns of birds and insects. Micro Aerial Vehicles (MAVs) are small robotic drones with cameras and built-in microphones and can be as tiny as a few centimetres (US Air Force Recruiting 2015). MAVs can work individually or in a swarm to infiltrate sensitive areas, where larger drones would be too bulky or noticeable, and transmit information back to a control centre. Considering that UAV surveillance has become more commonplace, it is not far-fetched for border patrol to further their surveillance efforts by employing MAVs. The MAVLab (nd) at the Delft University of Technology in The Netherlands specialises in micro and nano-air vehicle research, as does Harvard's Microrobotics Lab, and departments within MIT.

Considering that this type of surveillance is designed to be incognito, the infringements upon privacy rights are flagrant. A goal of MAV aeronautical engineering is for the device to be capable of accurately landing on the human skin, and potentially collecting DNA samples or detecting chemical radiation (Office of Communications 2012). Policy relating to the use of these machines at transit points needs to be discussed at greater lengths with more transparency as to their capabilities and applications, allowing for an interdisciplinary approach to important regulation for technology that has unprecedented consequences.

3.3 Human rights implications

The effects of utilising fourth revolution technologies will continue to be a morally-charged issue, and voters without a detailed understanding on matters of privacy versus security will remain in a haze of doubt. At present, advancing technologies are contributing to an already dehumanising and under-resourced flood of immigration casework. Steven Levy, a tech correspondent for WIRED, addressed the human rights concerns that arise when painstakingly omniscient technology begins to infiltrate sensitive situations:

Families are not part of the Anduril [executives'] thought processes. They're fulfilling what the government wants done and they aren't getting involved in the politics. But what we are learning is that technology is politics. They consider themselves as patriots doing this for the government, but you can't do this without dealing with the implications of your technology (CNBC 2018).

Under the Trump administration's 'zero tolerance' immigration policy, close to 3 000 children were forcibly separated from their parents and placed in shelters – some with extremely poor conditions – or foster care (Office of Inspector General 2019:1).

Reviewing the equipment used by the border patrol agents, it is clear that militarising the border means far more than just deploying troops manned with heavy artillery weaponry. The same technology being used to hunt high-profile enemies of the state and internationally infamous

terrorists is being used to peer over state lines and detect the movement of migrants in neighbouring countries. Operating under the guise of national security is an ethos-driven argument for patriotism, yet the implications of surveillance with piercing accuracy include dangerous human rights violations.

As explained by Lyon (2007: 7), if the objective of surveillance is social sorting, then systematising classifications of people merely precedes unequal treatment. In the case of migration, this translates to either granting or rejecting access to state territory, visa privileges or asylum status. Digitising the border via artificial intelligence, integrated IoT communications networks, and biometric data collection can lead to formulaically differentiating between which people governments consider to be more valuable. Artificial intelligence is already sorting cargo in the EU, as explained by Sven Suurraid, head of the customs department for the Estonia Tax and Customs Board: 'It's nice to have very modern railway X-rays but the analysis of the images must develop to the next level, not made by humans. Our future is in pairing machine learning and artificial intelligence to check these pictures' (Lewington 2018). Will humans be processed in the same way?

When machine-learning outputs include solutions based on one-dimensional algorithms, the risk lies in an inability to programme the essence of morality into a technological system, leaving all other dimensions related to human rights behind. Bowling and Sheptycki (2015: 151) argue that law enforcement and all of its peripheral branches will increasingly rely on technology, but officers must remember that 'a device is more than just a technological tool and should be seen as an important component in the process of transnational policing and in the deployment of specific rationalities in the governance of security'. As suggested, technology is a mere component to the larger picture, as there are many other sensitive factors at play when dealing with migrants, refugees and asylum seekers. A state's border security strategy should incorporate cooperative neighbourly relations in order to achieve the common goal of filtering out smugglers and terrorists, all the while stimulating business, cross-cultural value sharing, and ensuring that all people have the right to be treated with dignity.

As in the case of all new technologies, its application is more important than the technological development itself. There are infinite examples of how technology has been used to help humankind, but it has only ever been accomplished with a person who values humanity driving the achievement.

4 The impact of digital walls and data-driven barriers on vulnerable groups

In the past, humans were responsible for managing tasks and risk along the border, meaning a conscious mind would make the final decisions. However, these tasks are now increasingly being carried out by machines, implying an algorithm may decide the future of a human's fate.

This part of the article examines the impact of border digitisation on individuals, particularly focusing on the discriminating effects pertaining to vulnerable individuals or groups. It explains how a machine can hold

biases and the extent to which algorithmic discrimination can be applied at the border. The interactions between facial recognition systems and vulnerable groups, including dark-skinned women, are the basis for this section, which explains how machines can impose discrimination and further disadvantage the most vulnerable groups in society.

A machine itself is not discriminatory, but machine-learning algorithms can be shaped to be so. Facial recognition is performed by automated facial analysis algorithms that are trained with datasets, which contain thousands of pictures of faces. By training the algorithm with those pictures it can learn to recognise and classify faces. A comparative study carried out by Buolamwini and Gebru (2018: 77-79) showed that some of the widely-used datasets are composed of samples where more than two-thirds of the images are light-skinned faces. Therefore, the algorithms trained with these skewed datasets will be much more precise in recognising light-skinned people over dark-skinned people. The study by Buolawinis and Gebrus not only reveals that the trained algorithms have problems correctly identifying dark-skinned people, but they also have a gender bias. Many women were wrongly detected as male or not recognised as human faces at all. Females were underrepresented in the dataset, which resulted in an average error rate for dark-skinned women as 34,7 per cent, whereby light-skinned males were misclassified by only 0,8 per cent (Buolamwini & Gebru 2018: 77-82).

These kinds of skewed datasets are not only used for facial recognition systems by tech companies, such as Apple installing facial recognition into their products, but also by the police to enforce the law. Consequently, public authorities make decisions based on these flawed systems. For instance, in some US states law enforcement uses a facial recognition system called Rekognition provided by Amazon (Cagle & Ozer 2018). Shortly after the publication of the Buolawinis and Gebrus study, the American Civil Liberties Union (ACLU) tested Amazon's software. The ACLU results were shockingly similar to those of the Buolawinis and Gebrus study, which tested facial recognition systems from other providers. ACLU's test proves that Rekognition was trained with a dataset predominantly made up of pictures of light-skinned people (Snow 2018).

Test results such as these triggered Amazon's shareholders to call for a bar on selling facial recognition systems to law enforcement. The shareholders were particularly concerned about civil and human rights violations (McFarland 2018). Wood (2018) points out in Amazon's official AWS Machine Learning Blog that Rekognition can be used to fight crimes such as human trafficking or child exploitation and that any unlawful use or harmful act towards someone with the software is prohibited. Facial recognition systems might have some positive uses and make several areas of work more efficient. However, even in lawful use and properly exercised by professionals, algorithms can be biased and, therefore, discriminatory.

Concerns about facial recognition systems and their impact on civil and human rights have already proven to be valid. The danger of such systems stems, on the one hand, from the issue of racial and gender bias. On the other hand, it lies in how this biometrical technology is used in practice. It can lead to unfair practices and discrimination due to biased profiling. Unfortunately, technologies have evolved so fast that legal regulations have not yet caught up, which is particularly important to observe in the US.

In the context of border management, facial recognition systems are most often used to conduct profiling. Profiling is a way of categorising individuals on the grounds of changeable or unchangeable characteristics. The collected data is converted into profiles and stored for a certain amount of time (European Union Agency for Fundamental Rights 2018a: 15-16). It is important to note that profiling, exercised either by humans or systems with an underlying algorithm, is always – consciously or unconsciously – biased. Algorithmic systems are biased because of previous learning experiences or from the database that trained the algorithm. Those biases influence the profiling assessment as well as the decision making (European Union Agency for Fundamental Rights 2018a: 18). Thus, there is a high risk for discrimination. In other words, profiling is unlawful if an individual or a group of people would be treated less favourably than another person or group in a comparable situation as a result of targeting due to subjective justification (Council Directive 2000/43/EU, Article 2, 2000). In addition, using a biased algorithm in a facial recognition system could lead to structural discrimination.

However, facial recognition systems are becoming standardised for profiling at most border checkpoints. There are two main reasons for conducting profiling in border management: first, to identify individuals. This is important in order to find out whether the subject is already known or not, and if there is already a history with that individual. Second, profiling is used to predict behaviour and to make decisions concerning the profile due to these predictions. This is especially important for security and law enforcement reasons, and even of greater importance if the subject is not yet known in the system. Such a presumption could be the likelihood of the person remaining in a country after their authorised stay has finished. With the presumptions regarding the subject generated from the system, border management has an additional tool to decide what kind of policing (proactive or reactive) is adequate for the situation.

In the EU Schengen zone, facial recognition is being tested for entry/exit situations. By collecting biometric data, policy makers hope to maximise security by minimising the falsification of travel documents and illegal stays. Augustin Diaz de Mera Garcia Consuerga (2017) from the European Parliament points out that security- and preventive-driven policing became more prominent after the increased mixed migration flows towards Europe in 2015 and several terrorist attacks – such as the 2016 Berlin attack when the police uncovered that one of the assailants had used 15 different identities.

Amassing vast amounts of personal data and conducting profiling are methods being more frequently used in combination with algorithms to create coded solutions for automated decision making (ADM). Algorithms with ADM have been a fixed part of our lives for a while now. One of the most common examples is the spam filter in every inbox (European Union Agency for Fundamental Rights 2018b). Sometimes an e-mail is moved to the spam folder by the algorithm, despite it being an e-mail that typically would not be regarded as 'junk mail'. The same thing happens when using ADM at border crossing points, especially when the algorithm contains racial and gender biases. A refugee woman could be wrongly detected as someone who has already applied for asylum and would therefore be rejected. ADM is applied frequently and the reasons why it is used could

turn out to be more dangerous than anticipated. This danger provides reason for legal regulation that must be kept up-to-date with technological developments.

The EU law is more developed than the US law regarding the regulation of profiling and ADM. Regulation (EU) 2018/1725 applies to personal data proceedings directly executed by an EU governing body, organisation or agency. This regulation allows the EU to collect and process intimate personal data if an EU body needs the data to fulfil its mandate. This usually applies in the context of security such as border management. In practice, this means that Frontex is only allowed to use ADM under certain circumstances. Therefore, in most cases Frontex is obliged to use profiling as an additional tool to gather information but not to make decisions solely based on this technology. This minimises the risk of vulnerable parties falling victim to a biased or incorrect algorithm.

In addition to Regulation (EU) 2018/1725, the EU also regulates profiling and ADM under the General Data Protection Regulation (GDPR). This is important because of the limitation on data mining and surveillance performed by private companies. The GDPR prevents the gathering of personal data in another context in addition to prohibiting the sale of that information to law enforcement. Under article 22 §1, GDPR (Regulation (EU) 2016/679, article 22) profiling is only accepted under the condition that the decision cannot solely be based on ADM and it shall not affect the data subject in a significant way. Even though article 22 §2 allows profiling under very specific circumstances, article 22 §3 restricts this profiling. It does so by referring to article 9 §1 GDPR, which regulates processing of special categories of personal data (Regulation (EU) 2016/679, article 9). These include, among other personal data, genetic data and biometric data, which are extremely sensitive because they remain unchanged for a very long period of time (Deutsches Referenzzentrum für Ethik in den Biowissenschaften 2019).

In situations such as border management, profiling can have a very serious impact on minorities or vulnerable groups such as dark-skinned women. Nonetheless, profiling is widely used in border management and in some countries even in combination with ADM (Osborne Clarke 2018). Facial recognition systems are not the only AI systems with algorithmic discrimination. In recent years more systems have developed similar problems. However, as a result of these other systems being largely used among different sectors, facial recognition systems have come under more prominent scrutiny than others. Nonetheless, the legal framework still has to keep up with the fast evolvement of new technologies, which is discussed in more detail in the next part.

5 Balancing security and human rights: Analysing the shifting policy and legal frameworks on digital walls and border surveillance

As discussed above, means of surveillance have greatly transformed since the beginning of the twenty-first century. What started as traditional, manual mechanisms rapidly shifted towards new, automated technologies,⁶ which have proven to be cheaper, faster and able to deliver thousands of terabytes of information and knowledge in a single chip. This

part first focuses on the shift in policy making that has taken place in response to the expansion of surveillance and biometric data collection in law enforcement, using the US and Europe as case studies. It addresses the risks and consequences of constant border surveillance and concludes with an analysis of the present legal framework and attempts to balance security and fundamental rights.

After the 9/11 attacks people's perceptions of privacy and security changed radically, not only in the US but worldwide. As a global political narrative began to focus on border control, civilian attention also began narrowing in that direction. Emergency driven policies transformed into organised intelligence, in which constant mass surveillance became necessary for law enforcement and national security. The increased number of surveillance mechanisms and high-profile biometric devices pending patent registration reflects this change in policy and mindset. Between 1970 and 1995 the US Patent Office granted fewer than ten patents involving facial recognition systems. From 1995 to 2000 it issued 20 such patents. Between 2001 and 2011 the number leapt to 633 (Donohue 2012: 410).

Emergency-driven policies, which tried to tackle problems once they materialised, became obsolete within policy making as governments shifted towards a risk-management approach, which focused on prevention as the main way to avoid terrorism, (non)-organised criminality and irregular migration.

In practice, however, the risk management approach often is not proportional to the limitations of rights it brings with it, consequently becoming too invasive (Degli Spotzi 2018: 79). With massive surveillance operations, there is a tendency to move from contextualised surveillance to a generalised surveillance through the collection of purely preventive information, carrying with it the respective violations of the fundamental right to privacy.⁷ From a human rights law perspective, this approach should incorporate a proportionality test, as it should analyse risks in accordance with overall risk tolerance and decide whether or not the limitation of civil liberties is warranted. Since border surveillance suggests a threat to privacy by enabling widespread surveillance and massive personal information storage in databases (Nissenbaum 2010), the privacy-security trade-offs must be carefully assessed. The so-called risk-management approach has inevitably taken us to profiling and uninterrupted data storage as common practices. Border agents have used profiling as a modern tool for identifying and categorising people in order to detect threats within the stream of border traffic through data mining, as explained in the previous part.

Establishing what a legitimate limitation of rights entails can be a daunting task. While surveillance for illegitimate reasons violates privacy, surveillance for legitimate purposes can also do so if the associated privacy harms are not proportional to the ultimate purpose (Latonero 2018: 149-161).

6 Automated technologies are those operating by automatic means, reducing the human intervention as an operator to a minimum.

7 Art 12 UDHR; art 8 ECHR; art 7 EU Charter of Fundamental Rights (ECFR).

In the current context of high migration flows, both border agents and governments have been accused of profiling (Panneta 2019) and of data retention⁸ as an abuse of privacy (Massé 2016). As explained in this article, efforts to increase biometrical identification systems are spreading fast around the world. Within biometric identification, there are two types that have been widely used (Donohue 2010: 414-415), namely, immediate biometric identification (IBI) and remote biometric identification (RBI). IBI is focused on a single individual, with a close-up, and it is used in particular for detention purposes in a government-owned area. RBI, on the other hand, gives the government the ability to determine the identity of multiple people, both in public spaces and at a far distance (Donohue 2010: 414-415). As part of the risk management approach, the federal government in the US has increasingly invested in RBI technologies to supplement its IBI capabilities (Donohue 2010: 414-415).

The legal nature of these two types of biometric identification is different. Whereas IBI involves notice and consent and is limited in its occurrence, RBI does not require notice or consent, as it is done in a continuous manner (Donohue 2010: 414-415). This distinction is especially important in the context of border management, since millions of people are crossing borders daily. Surprisingly – or perhaps not – all this personal information is stored in servers that are not accessible to the public, raising concerns about data privacy and potential misuse. The same concerns apply to facial recognition technology (FRT), as this allows governments to observe and retain data in public spaces. China started a national surveillance system comprising 200 million cameras, with plans to have 300 million cameras in place by 2020 (Mozur 2018). China is also using its mass surveillance capabilities to create a system of ‘social points’; the government is tracking people’s habits, like online shopping behaviour or smoking in public, to grant and detract from civic rights and opportunities (McDonald 2018).

In response to all these privacy concerns, each government’s script is often the same: National intelligence agencies promise to minimise terrorism and crime with the retention of our personal data. States often defend this by saying that it is not an intrusion into our private sphere. However, evidence such as the Snowden revelations has shown that there is a permanent state of surveillance by states of people both at borders and within them (Greenwald 2013).

As far as mass data retention is concerned, Frank La Rue, the former UN Special Rapporteur on Freedom of Expression, acknowledged:

National data retention laws are invasive and costly, and threaten the rights to privacy and free expression ... [M]andatory data retention laws greatly increase the scope of state surveillance, and thus the scope for infringements upon human rights. Databases of communications data become vulnerable to theft, fraud and accidental disclosure (A/HRC/23/40).

8 Art 5(e) GDPR: [Data should be stored for] ‘no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes’.

This shows not only how we are subject to mass surveillance, but also the risks of such mass surveillance. The legislative framework in place with regard to data retention contains many shortcomings. These shortcomings increase the risk of human rights violations, as they allow for the use of data to limit access to certain territories, curtail freedom of expression and hamper personal data sovereignty due to the creation of long-lasting personal files. These not only present an immediate risk, but raise concerns for greater risks in the future, depending on the judgment of those in power.

There are no worldwide legal provisions that regulate and protect the processing and storage of biometric data. Instead, the overall trend is to include the collection and use of biometric data within the framework of personal data protection and domestic privacy laws (Council of Europe 2018). The intangible nature of data poses a complicated dichotomy. In practice, data flows freely across geographic borders, but the territorial scope of data protection laws is restricted. While border digitisation undeniably affects privacy and data protection, practice shows that the lack of territoriality of the internet also poses grave concerns for the right to privacy. According to Justice Abella from the Supreme Court of Canada, '[t]he internet has no borders – its natural habitat is global' (*Google v Equustek* 2007). Collected data from government surveillance similarly is borderless.

In the US only a handful of states currently regulate biometrics within their legal frameworks,⁹ and there is no framework regulating patents whatsoever. Unlike in Europe, privacy is not a fundamental right in the US, where it is often balanced against the Fourth Amendment. The 1974 US Privacy Act regulates how the federal government holds personal data and stores it. However, it is important to know that there currently is no single principal data protection legislation in the US. Furthermore, at the jurisdictional level, the courts use the reasonable expectations of privacy principle, which is an element of privacy law that determines in which places and during which activities a person has a legal right to privacy. Whereas this principle is used to protect against undue interference in private life, it makes the right to privacy dependent on the situation and context, giving the impression that fundamental rights are dependent on a person's circumstances.

In Europe, on the other hand, the GDPR entered into force in May 2018 and represents the culmination of Europe's efforts to be at the forefront of data protection. The scope of application of this law is limited to private organisations, companies and individuals processing personal data of EU citizens or foreigners based in the EU. Described as a very sophisticated law (Guido Raimondi 2018), the GDPR introduced a new sanctionatory structure, in which non-compliance can lead to fines of up to €20 million or 4 per cent of a company's annual worldwide turnover (GDPR 2018, art 83.5). This law applies to subjects 'whatever their nationality or place of residence' (GDPR 2018, recital 14) within the EU. It is of utmost importance since it regulates the information that could fall into the hands of private companies within the context of border-crossing. In addition, Directive (EU) 2016/680 is used for applying the GDPR when law

9 Illinois, Texas and Washington, for example, have passed biometric privacy laws subsequently since 2008.

enforcement is involved. It regulates the processing of personal data of natural persons by competent authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences (GDPR 2018, recital 19).

The GDPR also provides a clearer definition of consent, which changed from merely 'freely given' to 'freely given, specific, informed and unambiguous'. This change was most likely prompted by the fact that privately-run companies, and sometimes governments, often hide behind the mask of consent to renounce any responsibility, as Facebook did in 2018 (*Federation of German Consumer Organisations (VZBV) v Facebook* (2018)).

In order for consent to be valid, data subjects must be given a genuine and free choice. This essentially eliminates forced consent within the borders of the EU. In other words, when two parties sign a contract and the one party has no way of declining consent without suffering a consequence, consent is fundamentally biased. This applies even more so to situations in which consent is not even explicitly given, such as in the context of border surveillance. As a consequence, the idea of consent as we know it today has led some academics to refer to consent as a myth (Degli Spotzi 2018: 177).

When the EU (as an institution) is collecting data, the regulation applicable is Regulation (EU) 2018/1725, which is fully in line with the GDPR. This regulation lays out the data protection obligations for EU institutions and bodies as they process personal data and develop new policies. It is enforced as soon as EU agencies come in contact with data. However, its scope is wider because of the protective mandate of such institutions. For example, it would regulate how Frontex deals with refugees' personal data.

In Europe article 8 of the European Convention for the Protection of Human Rights and Freedoms (ECHR) on the right to respect for private and family life is central to the privacy-security trade-off debate. The European Court of Human Rights (European Court) has balanced article 8 with conflicting interests such as private property and national security. If a state were to limit article 8, this interference would have to be 'necessary in a democratic society', meaning that there must be a 'reasonable' 'pressing social need' (Council of Europe 2019) for such intrusion in the private sphere.

This privacy-security conflict is addressed in cases such as *Klass & Others v Germany*. In this case the Court held that there had been no violation of article 8, finding that the German legislature could draft legislation empowering the authorities to monitor people's correspondence and telephone communications without having to inform them. This case was made on the grounds of national security and public interest. In *Malone v United Kingdom*, however, the Court held that there had been a violation of article 8 when the government tapped communications, and constantly monitored them without reasonable clarity or scope.

Similarly, on 6 October 2015 the European Court of Justice (ECJ) issued its judgment in the case of *Schrems v Data Protection Commissioner*, declaring the European Commission's Decision 2000/520/EC invalid, which allowed transfers of personal data from the EU to the US. While the

Schrems judgment only directly concerns data transfers from the EU to the US, its ramifications may indirectly affect cross-border data transfers more generally. In the same way, the ECJ issued Opinion 1/15 on 26 July 2017, and as interpreted in the *Schrems* judgment, the transfer of data to a third country became possible only if such country ensures an adequate level of protection.

In the *US v Jones* case (2012) the US Supreme Court established that monitoring a car through the use of GPS constitutes a violation of the Fourth Amendment, the principle that protects people against unreasonable searches. The Court ruled that the GPS monitoring was disproportionate in time and space and it was a trespass of Jones's personal effects. Similarly, in *US v Maynard* (2010) the Court established that attaching a GPS to a person's vehicle without a warrant constitutes a violation of the Fourth Amendment. The Court stated that 'a person who knows all of another's travels can deduce whether he is a weekly church goer, an unfaithful husband ... and not just one such fact about a person but all such facts'.

Furthermore, while border surveillance can potentially be a threat to civil liberties, it is particularly apparent that those who have the power to control surveillance are the ones who can abuse it of their own volition. Reports claim that in 2016 Donald Trump's personal lawyer allegedly met with a KGB operative in Prague, despite the fact that his passport holds no proof of entry to the Czech Republic (Stone and Gordon 2018). If accurate, this case may show how border surveillance, rather than merely following traces based on stamps within passports, can function as a means of transparency. Technology allows tracking to be done independently of there being evidence of a border having been crossed or not, which may result in holding elected officials accountable. Not surprisingly, border technology and surveillance is a controversial political issue, and the next part examines this political dimension in more detail.

6 Populism and digital walls: Analysing the political challenges to implementing human rights-friendly border technologies

Political will heavily influences the likelihood of border technology complying with human rights obligations, and thus determines whether smart borders amount to smart solutions. Therefore, this part examines the political playing field, focusing on the influence of right-wing populist parties. The emphasis is on the EU, but events in this region reflect the growing international support for populist leaders (Kyle and Gultchin, 2018).

Going forward the rise of populism could present a challenge to human rights protection in border technology. A central contention of this article is that the rise of the populist far-right in Europe is playing into the securitisation culture surrounding migration. The proliferation of securitisation in the EU coincides with the militarisation of its borders. It has been argued that these phenomena are inter-related as an enhanced focus on security at the border can justify the use of militaristic paraphernalia. Granted, numerous factors contribute to the increased use of security technologies on the EU's external borders, including the economic interests of arms traders and the fear of terrorism since 9/11.

Nonetheless, the connection between securitisation, militarisation and right-wing populists is worthy of consideration. It must be stated from the outset that the militarisation of borders predates the rise of right-wing populism. Moreover, until recently right wing populists did not wield any direct control over the EU so they did not have a direct impact on policy relating to the EU's external border. However, the trend demands attention for a number of reasons. First, right-wing populists are gaining international traction. Second, right-wing populist rhetoric extols the benefit of strong borders; and through repeating this, they encourage a shift to the right among other political actors.

This article argues against the idea that populism is irreconcilable with technology and instead contends that populist solutions are inextricably linked to emerging technologies. To further elaborate on the connection between rising right-wing populism in Europe and border technologies, this part first discusses a definition of right-wing populism and the centrality of borders in their politics; second, it addresses the significance of social media and the influence of populist discourse across the political spectrum; and, finally, outlines the relationship between securitisation and militarisation of migration.

In Europe, borders have become a political priority due to an unanticipated surge in immigration. Conflicts in the European neighbourhood and the Middle East led to an influx of migration over the past decade, peaking in 2015 and 2016 (Johansson-Nogués 2018: 529). A 2016 Commission Communication stated that the number of migrants globally in 2016 represented the most severe refugee crisis since World War II (European Commission 2016). The sheer volume of people entering the EU and the dangerous routes taken (via boat and on foot) undeniably resulted in a humanitarian crisis (Neville, SY, Rigon, 2016: 8). This crisis led parties across the political spectrum to look for ways to respond. The European Parliamentary Committee on Civil Liberties, Justice and Home Affairs repeatedly called for the creation of legal routes into the EU (Luyten and González Díaz 2019), whereas more conservative parties called for stricter border control.

Quite apart from these two responses was the response of right-wing populists. These groups not only call for stricter immigration controls but also argue that settled immigrants are corrupting the values and culture of their respective nations. Recently, the European Commission declared the migration crisis over, and the Commissioner for Migration, Home Affairs and Citizenship noted that irregular arrivals are now lower than before the crisis (European Commission Press Release Data Base 2019). Nonetheless, populists continue to warn against rising migration (Roth 2019). A 2011 Chatham House report (Goodwin 2011: x) stressed that anti-immigration sentiment is a defining characteristic of right-wing populism:

These parties share two core features: They fiercely oppose immigration and rising ethnic and cultural diversity, and they pursue a populist 'anti-establishment' strategy that attacks mainstream parties and is ambivalent if not hostile towards liberal representative democracy.

One reason why border control is so important to populists is that it symbolises the exercise of state sovereignty. States traditionally held the power to decide how many people could enter their territory, as well as the processes for crossing the border. However, in a globalised world, states no

longer have boundless discretion. Rather, they are restricted by international obligations and commitments. These include principles of international law such as *non-refoulement* protections (OCHRa 2018) guaranteed under international humanitarian law and standards set out in international human rights treaties (OCHRb 2018). Furthermore, states in the Schengen area pledged to cooperate with others in the area regarding how to manage the external frontier of the EU. Populist parties equate this diminution in the ability of the state to make independent decisions regarding migration, as an imposition on state sovereignty.¹⁰

Other features of populist agendas may seem unrelated to borders and migration at first glance. However, on further inspection the connection becomes apparent. For example, an identifying characteristic of populist parties is that they claim to represent 'the people'. Advocating greater accountability and responsiveness from democratic systems would seem to be a laudable aspiration. However, the populist conception of democracy leaves no room for pluralism. They portray 'the people' as a homogenous whole; the people are not just 'demos'; they are also 'ethnos' (Pasquino 2007: 16). In their 2017 World Report, Human Rights Watch (Roth 2017) noted:

Throughout the European continent, officials and politicians harken back to distant, even fanciful, times of perceived national ethnic purity, despite established immigrant communities in most countries that are there to stay and whose integration as productive members of society is undermined by this hostility from above.

These points go some way towards explaining why borders are a site of utmost concern for populists. In populist discourse, migration is more than a question of policy; it is a question of transcendental import. Borders take on spiritual significance, in that they represent an answer to the most essential of human questions, 'why do we suffer?':

Populism employs a secularised version of the myth of the fall of man to explain suffering as something more palatable to the sufferer. Things have gone wrong, suffering has come into the world with the others (the immigrants, the political elite, the established media), and what we need to do now is return to the paradisiacal State that existed before the fall (Hendricks & Vestergaard 2019: 93).

While they have built their rhetoric and agenda in this vein, populist parties have relied on emerging technologies to garner support. It has even been argued that the formats of certain sites encourage more radical perspectives (Bartlett 2018). Social media sites provide an ideal platform for populist parties. Simple messages sell online and populist outlooks attract more attention online than anything in the 'watery centre ground' (Bartlett 2018). Hendricks and Vestergaard (2019: 88-89) write:

Populism is an efficient media strategy that plays on emotions. The narrative structure of us-versus-them, with the others being villains, is efficient when it comes to mobilising anger or fear. News stories that provoke anger (ie, indignation) and fear have a much greater tendency to go viral and suck attention on social media.

10 With that said, populist parties may be willing to support European Union cooperation if the goal is to reduce all immigration, via a method they agree with.

The fault here cannot be placed squarely on new social media platforms. Instead, these platforms just exacerbate innate human tendency to gravitate towards stories that affirm one's own world view. This tendency accounts for the success of misinformation online. As Hendricks and Vestergaard explain (2019: 80), cognitive dissonance and selection bias play an important role in this context. These methods of sharing and receiving information contribute to the polarisation of the political spectrum. Etzioni (2018: 131) explains that causes of the success of populism among traditional communities include 'fragmentation of the news, gerrymandering, self-segregation, and political polarisation'. This media landscape contributed to the growth of the populist right across Europe by reinforcing outlier perspectives.¹¹

The success of right-wing populist agendas online has an impact 'in real life'. Notably, even where right-wing populists have not gained a majority, the presence of support for right-wing populists in the political arena pushes centre parties further to the right. An example of this is the German tightening of border control following Chancellor Angela Merkel's initial open response to the migration crisis (Balfour 2016: 48). It demonstrates how the influence of populist candidates changes the political arena, irrespective of whether they directly hold power or not. A 2016 European Policy Centre report (Balfour 2016: 3) argues that in the current interconnected and globalised world, the impact of domestic policy discourse extends beyond state borders. Therefore, right-wing populist groups influence EU foreign policy and border management, even though they have not enjoyed parliamentary success in all EU member states.

If one accepts that the growth of populism affects the political arena, this leads to the question of how populism will affect border policy. Right wing populism contributes to an atmosphere of securitisation which can contribute to border militarisation. This is a significant factor to take into account when discussing border technologies, because where technologies are rolled out as a part of border militarisation rather than as a part of a project with humanitarian intentions, this affects the priority given to human rights.

An atmosphere of securitisation has crept over Europe. In this context, contemporary politics often presents a dichotomy between security and human rights. For example, as was discussed in the previous part, increasing data surveillance is justified by the ends of security and peace. Granted, security plays a role in every state, but security cannot be used as a trump card nor can it be used to justify disproportionate responses to threats. Some security concerns pertaining to migration are warranted but right-wing populists play on the fears of the electorate by framing security as the predominant lens for viewing questions relating to borders.

Right-wing populists cannot be blamed for the securitisation of migration. Rather, they are merely a catalyst in a pre-existing discourse.

11 There are other factors at play. For example, populist politicians may spend more time on the ground speaking with their constituents; they express the rage that large demographics of society feel towards the liberal system of globalisation; and people may feel drawn to more radical parties as the traditional left and right hover at the centre, resulting in a deficit of meaningful opposition. Furthermore, it may just be that many people still hold xenophobic bias.

Indeed, parties of different persuasions have long framed migration policy through security terminology. Lazaridis and Konsta (2015: 184) explain:

Security concerns have topped western political agendas since the attacks of 9/11, ... Included among the non-military threats to state security is migration, the idea being that liberal migration regimes advance cross-border risks – for example, that of terrorism – while more restrictive regimes minimise such threats and improve national and societal security.

The EU itself has played into the securitisation of migration. The 2016 European Agenda on Migration links the control of migration to security by explicitly stating that migration and border management will be a component of Common Security and Defence Policy missions ongoing in Niger and Mali (Davitti 2019: 47).

Notwithstanding the pre-existence of the securitisation paradigm, it nonetheless can be argued that populist parties are unique in the extent to which they exploit the othering of migrants to further their own political agenda. Lazaridis and Konsta point out how Golden Dawn in Greece and the British National Party in the United Kingdom ‘take advantage of the securitisation of migration’ (Lazaridis and Konsta 2015: 185) and how, ‘via populist actions, exclusionary practices are promoted through the construction of Otherness’ (Lazaridis & Konsta 2015: 185). Right-wing populists could push the discourse even further to the right which could in turn lead to more brutal approaches to border management.

But how does the paradigm of securitisation translate into the militarisation of borders? Or more succinctly, how could the rise of populism lead to the militaristic implementation of new border technologies? At first glance it may seem that right-wing populists are opposed to technologies on the border. Right-wing populists are often associated with crude tangible measures, such as building physical border walls. For example, President Trump and Viktor Orbán, Prime Minister of Hungary, are famous proponents of wall building (McTague 2017). Moreover, populist movements harken back to imagined glory days and this atavism seems at odds with the progression of technology. However, this view is overly simplistic. The populist leader of the US, President Trump, has invested in additional border security including new emerging technologies, albeit only after the idea was promoted by other Republicans (Cowen 2019). This demonstrates that populists’ border policy is not mutually exclusive with emerging technology. This conclusion is corroborated by the fact that populists rely heavily on social media to consolidate their support, as was discussed above.

It may be argued that the militarisation of the EU external border is already taking place. Private military and security companies are already reaping the benefits of a culture of fear (Davitti 2019), and right-wing populism serves to fan the flames of this fear. Kraska (2007: 503) defines militarisation as

a set of beliefs, values, and assumptions that stress the use of force and threat of violence as the most appropriate and efficacious means to solve problems. It emphasises the exercise of military power, hardware, organisation, operations, and technology as its primary problem solving tools.

This phenomenon that is taking place on the EU border as ‘security threats’ (Behr 2013) are framed to justify militaristic security methods

(Davitti 2019: 38). One indication that the external border of the EU is being militarised is that European military contractors, including Thales, EADS, Finmeccanica and Talos, benefit from producing technological equipment for border security (Jones & Johnson 2016: 5). Furthermore, during the migration crisis civil society called out the military style approaches of Frontex (Buxton 2016).¹²

While right-wing populism grows increasingly popular, there simultaneously is a rise in border militarisation, partly as a result of securitised discourse. It is the contention of this article that this combination could increase the potential of migrants' human rights being abused via new technologies. That is, unless developments in border technologies are monitored and leaders are made accountable for when these developments compromise the dignity of any person.

7 Conclusion

The application of new technologies in our daily life is unstoppable. As seen in this article, it can be for the good and for the bad. Due to a lack of knowledge about the workings of algorithms and missing regulations regarding transparency, technology is applied without necessarily knowing what harm it can do. Groups, especially those that are not on the frontlines of the fourth revolution and participating in the coding process, are left behind when it comes to knowing how the algorithm perceives them. Usually groups that are already vulnerable are also targeted by the bodiless algorithm. The most targeted group are dark-skinned people, especially women. In the most defenceless situations, such as at border crossing points, when applying for asylum an algorithm can not only discriminate against someone, but also massively violate other human rights. Therefore, it is more important than ever to be critical of new technologies and not to use them only because we can produce these technologies.

We are currently experiencing a shift in how security policies are made around the world. This shift carries the paradox that in order to have more security, one must trade off one's privacy. The tools theoretically used to fight terrorism and crime are the same as those used to scrutinise civilians, while convincing them that such tools are necessary and indispensable. In the long run, even when there are security-privacy trade-offs, these must be carefully assessed and weighted. As we are watching how regions shift towards a risk management approach, we will potentially witness limitations to civil rights and liberties.

For better or for worse, technology travels faster than law. Some laws that regulate privacy and data protection were created in the 1970s, such as the US Privacy Act, and have been proven to be outdated and insufficient to protect citizens against undue interference by states, and even private companies, that analyse and store such data. Although laws regulating privacy protection in Europe are a favourable step towards more data security, the mere definition of consent may have to be amended

12 It should be noted that the European Commission, in response to a parliamentary question, stated that Frontex bears no similarity to promoting the militarisation of the EU (Papadakis 2016; European Commission 2017).

worldwide. Until now, consent has operated as a legitimate basis for personal data processing and practice shows that this definition is not enough (Gonzalez Fuster 2018). The common understanding of consent needs to be revisited, as we know what happens when we agree to disclose certain types of personal information, but not what happens when we do not.

As of now, the EU is implementing adequate legal protection with Regulation (EU) 2018/1725. Until more advanced artificially-intelligent systems, such as dynamic algorithms, are applied in law enforcement, the regulation will not provide the needed protection that is required and it will only be a question of time until new types of machine discrimination occur or new ways of misusing the current technology are found. It could be that facial recognition systems will be used in a wide range of situations in the near future, such as to identify individuals at protests or in the context of border management. This can have negative effects: Individuals will be screened long before they arrive at the actual border and the decision about whether they are allowed to enter will be made in advance. This new way of using profiling may be justified through security and prevention reasons. In cases such as the Berlin truck bomber, hypothetically it could have prevented terrorist attacks and saved lives. However, in other circumstances, if policy makers decide to close borders due to predictions from algorithms, this might have negative effects, especially for the security of people travelling in large migration flows.

Alongside the legal framework, which must be up to date with technologies and include different means of application to prevent unlawful profiling and discrimination, there is also a need to fight bias and profiling on different levels in society, so as to prevent the feeding of human bias to algorithms. To the same end, algorithms have to be written by a heterogeneous team. Additionally, the algorithm should be trained using wider and more diverse datasets, gathered through different providers from all over the world. Furthermore, law enforcement units need to be diverse and specifically trained to become aware of their own biases and to learn how to regulate them. There is also a need for awareness about the shortcomings in algorithms. Summarily, a diverse society is a prerequisite. Diversity brings more knowledge, which results in more empathy. If that can be achieved, there automatically will be less bias in human decisions as well as less implemented bias in algorithms – therefore, greater data protection.

If the prospect of more diversity evokes hope about the potential positive human rights implications of border technology; then the shift in politics towards othering of migrants provides ample reason for pessimism. As was stated, populists may not have directly contributed to border policies but they do feed into the paradigm of securitisation. This article concludes with a warning. Going forward, technological solutions may seem like a more humane option than building physical barriers, but there are an array of human rights concerns associated with border technology, as laid out in this article. The aim of emerging border technology is not contradictory to the populist approach to borders. In fact, they can be complementary. If right-wing populist discourse continues to slowly push policy to the right in Europe, it increases the likelihood of border technologies being used in a manner that does not enshrine the dignity of migrants. As the EU gets ready to begin its new

mandate, it is worth remembering that new border technologies do not exist in a vacuum. Rather, how they are applied reflects political agendas. This lesson is as true in other regional contexts as it is in the EU. Ultimately, technology will change the way in which borders are managed across the world. It will impact sovereignty, migration routes, freedom of expression, privacy, surveillance and more. For this reason, considerate leadership is needed. Furthermore, it is the responsibility of scholars, human rights professionals and the media to highlight these emerging technologies and the consequences they have on vulnerable groups.

References

- Amoore L (2013) *The politics of possibility: Risk and security beyond probability* NC: Duke University Press
- Anduril (nd) *The lattice platform*, available at <https://www.anduril.com/lattice-ai> (last visited 12 April 2019)
- Angelescu I & Trauner F (2018) *10 000 border guards for Frontex: Why the EU risks conflated expectations* European Migration and Diversity Programme, available at http://www.epc.eu/documents/uploads/pub_8745_frontex.pdf?doc_id=2048 (last visited 10 April 2019)
- Arnold C (2010) *TSA to expand use of full-body scanners* National Public Radio, available at <https://www.npr.org/templates/story/story.php?storyId=122289282> (last visited 12 April 2019)
- Balfour R (2016) 'Europe's troublemakers The populist challenge to foreign policy' European Policy Centre, available at http://www.epc.eu/documents/uploads/pub_6377_europe_s_troublemakers.pdf?doc_id=1714 (last visited 16 April 2019)
- Bartlett J 'Why is populism booming? Today's tech is partly to blame' *The Guardian* 29 November 2018, available at <https://www.theguardian.com/commentisfree/2018/nov/29/populism-tinder-politics-swipe-left-or-right-unthinkingly> (last visited 18 April 2019)
- Behr T et al (2013) 'The maritime dimension of CSDP: Geostrategic maritime challenges and their implications for the European Union' Study Directorate General for External Policies, European Parliament, available at [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433839/EXPO-SEDE_ET\(2013433839_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433839/EXPO-SEDE_ET(2013433839_EN.pdf) (last visited 13 June 2019)
- Bier D & Feeney M (2018) *Drones on the border: Efficacy and privacy implications* CATO Institute, available at <https://www.cato.org/publications/immigration-research-policy-brief/drones-border-efficacy-privacy-implications> (last visited 15 April 2019)
- Biometrics and Technologies Council of Europe, available at https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Biometrics_technologies_v2.pdf (last visited 10 April 2019)
- Bowling B & Sheptycki JWE (eds) (2015) *Global policing and transnational law enforcement* Sage Publications Ltd
- Bowling B, Marks A & Murphy C 'Crime control technologies: Towards an analytical framework and research agenda' in R Brownsword & K Yeung (eds)

- Regulating technologies: Legal futures, regulatory frames, and technological fixes* (2008) OR: Hart Publishing 41(2018)
- Buolamwini J. & Gebru T 'Gender shades: Intersectional accuracy disparities in commercial gender classification' (2018) 81 *Journal of Machine Learning Research* 77, available at <http://proceedings.mlr.press/v81/> (last visited 15 April 2019)
- Broeders D 'A European "border" surveillance system under construction' in H Dijstelbloem & A Meijer (eds) *Migration and the new technological borders of Europe: Migration, minorities and citizenship* (2011) London: Palgrave Macmillan 40
- Broeders D 'The new digital borders of Europe: EU databases and the surveillance of irregular migrants' (2007) 22 *International Sociology*, available at <https://doi.org/10.1177/0268580907070126> (last visited 12 April 2019)
- Cagle M & Ozer N 'Amazon teams up with government to deploy dangerous new facial recognition technology' *American Civil Liberties Union* 22 May 2018, available at <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new> (last visited 13 May 2019)
- Ceyhan A 'Technologization of security: Management of uncertainty and risk in the age of biometrics' (2008) 5 *Surveillance and Society*, available at <https://doi.org/10.24908/ss.v5i2.3430> (last visited 9 April 2019)
- Chishti M & Bergeron C 'Post-9/11 policies dramatically alter the US' (2011) *Immigration Landscape*, Migration Policy Institute, available at <https://www.migrationpolicy.org/article/post-911-policies-dramatically-alter-us-immigration-landscape> (last visited 12 April 2019)
- CNBC 'These virtual walls could be the cheaper and more effective answer to Trump's \$5 billion border wall' (2018), available at <https://www.cnn.com/video/2018/12/14/this-border-town-doesnt-want-trumps-wall-but-a-silicon-valley-virtual-wall-could-stand-strong.html> (last visited 14 April 2019)
- Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180
- Cowen R 'Beyond Trump's wall: Congress tackles border security' *Reuters* 30 January 2019, available at <https://www.reuters.com/article/us-usa-shutdown-negotiators/beyond-trumps-wall-congress-tackles-border-security-idUSKCN1PO1ON> (last visited 23 April 2019)
- Davitti D 'The rise of private military and security companies in European Union migration policies' (2019) 4 *Business and Human Rights Journal*
- Department of Homeland Security (2005) 'Fact Sheet: Secure border initiative', available at www.dhs.gov/xnews/releases/press_release_0794.shtm (last visited 10 April 2019)
- Deutsches Referenzzentrum für Ethik in den Biowissenschaften [DRZE] (2019) 'Genetische Daten' translated by author DRZE, April, available at <http://www.drze.de/im-blickpunkt/praediktive-genetische-testverfahren/module/genetische-daten> (last visited 6 April 2019)
- Diaz de Mera Garcia Consuerga A 'Smarter borders for Europe' *European Parliament* 25 October 2017, available at <https://www.youtube.com/watch?v=J5qljEodBMM> (last visited 13 April 2019)
- Donohue K 'Technological leap, statutory gap, and constitutional abyss: Remote biometric identification comes of age' (2012) *Georgetown University Law Review* 1, available at <https://www.eff.org/pages/iris-recognition> (last visited 15 April 2019)

- Elbit Systems 'Elbit Systems presents Groundeye™: A new revolutionary line of advanced EO ground surveillance systems for wide-area focused and persistent intelligence gathering' (2016), available at <https://elbitsystems.com/pr-new/elbit-systems-presents-groundeye/> (last visited 11 April 2019)
- Elbit Systems (nd) 'Company profile: Next is now', available at https://elbit-systems.com/media/Next-is-Now_Booklet_General.pdf (last visited 18 April 2019)
- Elbit Systems (nd) 'Home', available at <https://elbitsystems.com/> (last visited 18 April 2019)
- EU Travel Information and Authorisation System 'ETIAS border security technologies' (2017), available at <https://etias.com/articles/etias-border-security-technologies> (last visited 12 April 2019)
- European Commission (nd) 'Biometric data', available at https://ec.europa.eu/home-affairs/content/biometric-data_en (last visited 14 April 2019)
- European Commission 'Answer given by Mr Avramopoulos on behalf of the Commission' Parliamentary Questions: Question reference: E-007071/2016' 11 January 2017, available at http://www.europarl.europa.eu/doceo/document/E-8-2016-007071-ASW_EN.html (last visited 19 April 2019)
- European Commission (2016) *Communication from the Commission to the European Parliament and the Council on the state of play of implementation of the priority actions under the European Agenda on Migration* (COM(2016) 85 final edn)
- European Commission (2018a) 'EU budget: €4.8 billion in security funding for a Europe that protects'
- European Commission (2018b) 'EU budget: Commission proposes major funding increase for stronger borders and migration', available at http://europa.eu/rapid/press-release_IP-18-4106_en.htm (last visited 10 April 2019)
- European Commission Press Release Data Base 'The European Agenda on Migration: EU needs to sustain progress made over the past 4 years' (2019), available at http://europa.eu/rapid/press-release_IP-19-1496_en.htm (last visited 18 April 2019)
- European Union Agency for Fundamental Rights (2018a) *Preventing unlawful profiling today and in the future: A guide* Luxembourg: Publications Office of the European Union
- European Union Agency for Fundamental Rights (2018b) *BigData: Discrimination in data-supported decision making* Luxembourg: Publications Office of the European Union
- Etzioni A 'Happiness is the wrong metric: A liberal communitarian response to populism' (2018) 11 *Library of Public Policy and Public Administration*, available at <https://www.springer.com/gp/book/9783319696225> (last visited 13 June 2019)
- Executive Office of the President of the United States (2019) 'Stronger border security: 2019 Budget Fact Sheet', available at https://www.whitehouse.gov/wp-content/uploads/2018/02/FY19-Budget-Fact-Sheet_Border-Security.pdf (last visited 11 April 2019)
- Fleming ST, Madden JM & Usery EL 'GIS applications for military operations in coastal zones' (2009) *ISPRS Journal of Photogrammetry and Remote Sensing* 64, available at http://scholar.google.pt/scholar_url?url=https://pdfs.semanticscholar.org/79c4/c469c72ba3237ea89147b2dc3fd5dc05ec75.pdf&hl=en&sa=X&scisig=AAGBfm1Tp8D3eaolHKSskvp_mpFkmtf5-og&noss1=1&oi=scholar (last visited 13 April 2019)

- Franko Aas K '“Getting ahead of the game”: Border technologies and the changing space of governance' in E Zureik & MB Salter (eds) *Global surveillance and policing: Borders, security, identity* (2005) UK: Willan Publishing 194
- Frontex (nd) 'Migratory Map', available at <https://frontex.europa.eu/along-eu-borders/migratory-map/> (last visited 11 April 2019)
- Gardiner B O'ff with your shoes: The brief history of airport security' (2013), available at https://www.wired.com/2013/06/fa_planehijackings/ (last visited 10 April 2019)
- Gemalto (nd) 'DHS's automated biometric identification system IDENT – The heart of biometric visitor identification in the USA', available at <https://www.gemalto.com/govt/customer-cases/ident-automated-biometric-identification-system> (last visited 17 April 2019)
- Greenwald G 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* 2013, available at <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> (last visited 11 April 2019)
- Goodwin M 'Right response understanding and countering populist extremism in Europe' (2011) *A Chatham House Report*, available at https://www.chathamhouse.org/sites/default/files/r0911_goodwin.pdf (last visited 16 April 2019)
- Haggerty KD & Ericson R 'The surveillant assemblage' (2000) 51 *British Journal of Sociology*, available at https://www.uio.no/studier/emner/matnat/ifi/INF3700/v17/bakgrunnsnotat/the_surveillant_assemblage.pdf (last visited 8 April 2019)
- Hendricks VF & Vestergaard M 'Reality lost: Markets of attention, misinformation and manipulation' Springer Open (2019), available at <https://www.springer.com/gp/book/9783030008123#aboutBook> (last visited 13 June 2019)
- Johansson-Nogués E 'The EU's ontological (in)security: Stabilising the ENP area and the EU-self?' (2018) 53 *Cooperation and Conflict*
- Hoffman M 'The future of border securing technology is here and it's terrifying' VICE (2016), available at https://www.vice.com/en_us/article/zngp34/the-new-frontiers-in-border-security-technology (last visited 13 April 2019)
- IDEMIA (nd) 'Video investigation: Analyzing video data to accelerate investigations', available at <https://www.idemia.com/video-investigation> (last visited 13 April 2019)
- Immigration & Checkpoints Authority 'Contactless, “breeze-through” immigration clearance trial at Tuas checkpoint' (2019), available at <https://www.ica.gov.sg/news-and-publications/media-releases/media-release/contactless-breeze-through-immigration-clearance-trial-at-tuas-checkpoint> (last visited 12 April 2019)
- Johnson J 'One hundred naked citizens: One hundred leaked body scans' Gizmodo (2010), available at https://gizmodo.com/one-hundred-naked-citizens-one-hundred-leaked-body-sca-5690749?utm_medium=sharefromsite&utm_source=gizmodo_copy&utm_campaign=top (last visited 13 April 2019)
- Jones R & Johnson C 'Border militarization and the rearticulation of sovereignty' (2016) 41 *Transactions of the Institute of British Geographers*
- Koslowski R & Schulzke M 'Drones along borders: Border security UAVs in the United States and the European Union' (2018) 19 *International Studies Perspectives*, available at <https://doi.org/10.1093/isp/eky002> (last visited 18 April 2019)
- Kraska PB 'Militarization and policing: Its relevance to 21st century police' (2007) *Policing* 1

- Kyle J & Gultchin L 'Populists in power around the world' *Tony Blair Institute for Global Change* (2018), available at <https://institute.global/insight/renewing-centre/populists-power-around-world> (last visited 18 April 2019)
- Latonero M 'Big data analytics and human rights' in MK Land (ed) *New technologies for human rights and practice* (2018) Cambridge University Press
- Landgericht Berlin (2018) *Klaus Muller v Facebook*
- Lazardis G & Konsta A (2015) *Identitarian populism: Securitisation of migration and the far right in times of economic crisis in Greece and the UK* London: Palgrave Macmillan
- Levy S 'Inside Palmer Luckey's bid to build a wall' (2018), available at <https://www.wired.com/story/palmer-luckey-anduril-border-wall/> (last visited 13 April 2019)
- Lewington L. 'Inside border technology' BBC Click (2018), available at <https://www.youtube.com/watch?v=laeSuws-mE0> (last visited 18 April 2019).
- Long D & Barrios D (nd) 'CBP's eyes in the sky: CBP's tethered aerostats keep watch for trouble from 10,000 feet' US Customs and Border Protection, available at <https://www.cbp.gov/frontline/frontline-november-aerostats> (last visited 12 April 2019)
- Luyten K & González Díaz S 'Legal migration to the European Union' European Parliamentary Research Service (2019), available at [http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635559/EPRS_BRI\(2019\)635559_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635559/EPRS_BRI(2019)635559_EN.pdf) (last visited 19 April 2019)
- Lyon D (2007) *Surveillance studies: An overview* UK: Polity Press
- Mason M (nd) 'Biometric breakthrough: How CBP is meeting its mandate and keeping America safe' US Department of Homeland Security, available at <https://www.cbp.gov/frontline/cbp-biometric-testing> (last visited 16 April 2019).
- Massé 'EU's "Smart Borders 2.0" increases risks of surveillance and privacy abuses' *Access Now* 2016, available at <https://www.accessnow.org/smartborders/> (last visited 5 April 2019)
- Marx GT 'Some conceptual issues in the study of borders and surveillance' in E Zureik & MB Salter (eds) *Global surveillance and policing: Borders, security, identity* (2005) UK: Willan Publishing 11
- MAV-lab (nd) 'Research topics', available at <http://mavlab.tudelft.nl/research-topics/> (last visited 17 April 2019)
- McDonald JOE 'China bars millions from travel for "social credit" offences' *Associated Press* 2019, available at <https://news.yhttps://www.apnews.com/9d43f4b74260411797043ddd391c13d8ahoo.com/china-blocks-travel-social-credit-offenses-113811546--finance.html> (last visited 1 April 2019)
- McFarland M 'Amazon shareholders call for halt of facial recognition sales to police' *CNN Business* 18 June 2018, available at <https://money.cnn.com/2018/06/18/technology/amazon-facial-recognition/index.html> (last visited 10 April 2019)
- Mctague T 'Hungary hardens immigration line' *Politico* 13 February 2017, available at <https://www.politico.eu/article/hungarys-new-hardline-immigration-scheme-viktor-orban-refugees-migration-crisis-europe/> (last visited 20 April 2019)
- Meyers DW 'Does "smarter" lead to safer? An assessment of the border accords with Canada and Mexico' Migration Policy Institute (2003), available at <https://www.migrationpolicy.org/research/does-smarter-lead-safer-assessment-border-accords-canada-and-mexico?pdf=6-13-0~1.pdf> (last visited 11 April 2019)
- Mittelstadt M et al 'Through the prism of national security: Major immigration policy and program changes in the decade since 9/11' Migration Policy Institute

- (2011), available at <https://www.migrationpolicy.org/research/post-9-11-immigration-policy-program-changes> (last visited 10 April 2019)
- Moura P & Garcia-Navarro L 'Brazil looks to build a 10,000-mile virtual fence' National Public Radio (2013), available at <https://www.npr.org/sections/parallels/2013/05/16/184524306/brazil-looks-to-build-a-10-000-mile-virtual-fence> (last visited 15 April 2019)
- Mozur P 'Inside China's dystopian dreams: AI, shame and lots of cameras' *The New York Times* 2018, available at <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> (last visited 1 April 2019)
- Mozur P 'One month, 500,000 face scans: How China is using AI to profile a minority' *The New York Times* 14 April (2019), available at <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> (last visited 14 April 2019)
- National Ocean Service 'What is LIDAR?' National Oceanic and Atmospheric Administration (2018), available at <https://oceanservice.noaa.gov/facts/lidar.html> (last visited 12 April 2019)
- Neville D, Sy D & Rigon A 'On the frontline: The hotspot approach to managing migration' Policy Department for Citizen's Rights and Constitutional Affairs European Parliament (2016), available at [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556942/IPOL_STU\(2016\)556942_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556942/IPOL_STU(2016)556942_EN.pdf) (last visited 18 April 2019)
- Nissenbaum H (2010) *Privacy in context technology, policy, and the integrity of social life* Stanford, CA: Stanford University Press
- Nixon R 'On the Mexican border, a case for technology over concrete' *New York Times* 20 June 2017, available at <https://www.nytimes.com/2017/06/20/us/politics/on-the-mexican-border-a-case-for-technology-over-concrete.html?module=inline> (last visited 13 April 2019)
- Northrop Grumman 'Northrop Grumman showcases comprehensive security solutions at ASIS International' (2004), available at <https://news.northropgrumman.com/news/releases/northrop-grumman-showcases-comprehensive-security-solutions-at-asis-international> (last visited 12 April 2019)
- Nowrasteh A 'The cost of the border wall keeps climbing and it's becoming less of a wall' Cato Institute (2019), available at <https://www.cato.org/blog/cost-border-wall-keeps-climbing-its-becoming-less-wall> (last visited 11 April 2019)
- OHCHRa 'The principle of *non-refoulement* under international human rights law' (2018), available at <https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/Protection.pdf> (last visited 18 April 2019)
- OCHRB 'What do we mean by "protection" for migrants?' (2018), available at <https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/Protection.pdf> (last visited 18 April 2019)
- Office of Communications 'Unravelling a butterfly's aerial antics could help builders of bug-size flying robots' John Hopkins University (2012), available at <https://releases.jhu.edu/2012/02/01/butterfly-study-could-help-builders-of-bug-size-flying-robots/> (last visited 17 April 2019)
- Office of Inspector General 'CBP has not ensured safeguards for data collected using unmanned aircraft systems' Department of Homeland Security (2018), available at <https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-79-Sep18.pdf> (last visited 17 April 2019)
- Office of Inspector General 'HHS OIG issue brief: Separated children placed in Office of Refugee Resettlement Care' US Department of Health & Human Resources (2019), available at <https://oig.hhs.gov/oei/reports/oei-BL-18-00511.pdf> (last visited 15 April 2019)

- Osborne Clarke 'Profiling and automated decision-making under GDPR' *Osborne Clarke* 5 September (2018), available at <https://www.osborneclarke.com/insights/profiling-and-automated-decision-making-under-gdpr/> (last visited 6 April 2019)
- Panetta G 'The US border patrol could be facing a lawsuit after 2 US citizens say they were detained for speaking Spanish' *Business Insider* (2018), available at <https://www.businessinsider.com/border-patrol-racial-profiling-lawsuit-2018-5/> (last visited 12 June 2019)
- Papadakis K 'Subject: "Militarisation of the EU" by the European border and coast guard' Parliamentary', Question to the Commission Question for written answer E-007071-16 to the Commission 26 September (2016), available at http://www.europarl.europa.eu/doceo/document/E-8-2016-007071_EN.html (last visited 19 April 2019)
- Papernot N et al (2017) *Practical black-box attacks against machine learning* Cornell University, available at <https://arxiv.org/pdf/1602.02697.pdf> (last visited 13 April 2019)
- Pasquino G 'Populism in democracy' in D Albertazzi & D McDonnell *Twenty first century populism: The spectre of Western European democracy* (2007) Hampshire: Palgrave Macmillan, available at https://books.google.es/books?hl=en&lr=&id=K2mADAAAQBAJ&oi=fnd&pg=PP1&ots=p8nr_PvWMG&sig=Sy5m4djHKNyEB57D8ve7REtaS10&redir_esc=y#v=onepage&q&f=false (last visited 16 April 2019)
- Pickering S & Weber L 'Borders, mobility and technologies of control' in S Pickering & L Weber (eds) *Borders, mobility and technologies of control* (2006) Netherlands: Springer 1
- Politifact at the Poynter Institute (2017) 'Triple ICE enforcement', available at <https://www.politifact.com/truth-o-meter/promises/trumpometer/promise/1440/triple-ice-enforcement/> (last visited 17 April 2019)
- Portilho T 'Our blind faith in AI is catching up to us' *Gulf Today* 27 March 2019, available at <https://www.gulftoday.ae/opinion/2019/03/27/our-blind-faith-in-ai-is-catching-up-to-us> (last visited 19 April 2019)
- Quanergy Systems 'Quanergy Explains Solid State LiDAR' YouTube 2018, available at https://www.youtube.com/watch?v=eiu_V4a6vm4 (last visited 12 April 2019)
- Quanergy Systems (nd) 'Mapping', available at <https://quanergy.com/mapping/> (last visited 11 April 2019)
- Raytheon (nd) 'JLENS', available at <https://www.raytheon.com/capabilities/products/jlens> (last visited 13 April 2019)
- Reed J 'Israel extends its high-tech barriers I FT World' *Financial Times* (YouTube) (2016), available at <https://www.youtube.com/watch?v=X9fe4m0UAg4> (last visited 18 April 2019).
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Ring T (ed) 'Frost and Sullivan forecasts expansion of border control biometrics' (2013) *Biometric Technology Today* 4, available at [https://doi.org/10.1016/S0969-4765\(13\)70069-9](https://doi.org/10.1016/S0969-4765(13)70069-9) (last visited 12 April 2019)

- Roth K. 'The dangerous rise of populism: Global attacks on human rights values' Human Rights Watch: World Report (2017), available at <https://www.hrw.org/world-report/2017/country-chapters/dangerous-rise-of-populism> (last visited 16 April 2019)
- Ruiz Benedicto A & Brunet P 'Building walls: Fear and securitization in the European Union' TNI (2018), available at <https://www.tni.org/en/publication/building-walls> (last visited 8 April 2019)
- Schengen Visa Info (2018) *Schengen Visa statistics for consulates – 2017*, available at <https://www.schengenvisainfo.com/statistics/visa-statistics-2017/> (last visited 17 April 2019)
- Schwab K 'The Fourth Industrial Revolution: What it means, how to respond' World Economic Forum (2016), available at <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> (last visited 17 April 2019)
- Snow J 'Amazon's face recognition falsely matched 28 members of congress with mugshots' American Civil Liberties Union 26 July 2018, available at <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28> (last visited 15 April 2019)
- Stone P & Gordon G 'Cell signal puts Cohen outside Prague around time of purported Russian meeting' 18 April 2019, available at <https://www.mcclatchydc.com/news/investigations/article219016820.html> (last visited 16 June 2019)
- Spotzi SD & Friedewalt M 'Aligning security and privacy' in *Surveillance, privacy and security* (2018) Routledge
- The Alan Turing Institute Data Ethics Group and the Independent Digital Ethics Panel for Policing (2017) *Ethics Advisory Report for West Midlands Police*, The Alan Turing Institute Data Ethics Group, available at https://www.turing.ac.uk/sites/.../turing_idepp_ethics_advisory_report_to_wmp.pdf (last visited 15 April 2019)
- The Economic Times 'Modi government plans 24x7 virtual fence along Indo-Pak border' 13 July 2018, available at <https://economictimes.indiatimes.com/news/defence/modi-government-plans-24x7-virtual-fence-along-indo-pak-border/articleshow/59969417.cms> (last visited 11 April 2019)
- Transport Security Administration 'TSA biometrics roadmap for aviation security & the passenger experience' (2018), available at https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf (last visited 5 April 2019)
- Travis A & Stewart H 'UK to pay extra £44.5m for Calais security in Anglo-French deal' *The Guardian* 18 January 2018, available at <https://www.theguardian.com/politics/2018/jan/18/uk-to-pay-extra-445m-for-calais-security-in-anglo-french-deal> (last visited 10 April 2019)
- US Air Force Recruiting 'US air force micro air vehicles' YouTube (2015), available at https://www.youtube.com/watch?time_continue=77&v=hPS9FFRUXo0 (last visited 16 April 2019)
- US Immigration and Customs Enforcement 'Who we are' (2018), available at <https://www.ice.gov/about> (last visited 12 April 2019)
- US Government Accountability Office 'Report to congressional requesters: Secure border initiative: DHS needs to strengthen management and oversight of its prime contractor' (2010), available at <https://www.gao.gov/new.items/d116.pdf> (last visited 13 April 2019)
- US Customs and Border Protection (nd) 'Trusted traveller programs: Frequently asked questions', available at <https://ttp.cbp.dhs.gov/faq> (last visited 12 April 2019)

Vallet E (2016) *Borders, fences and walls: State of insecurity?* NY: Routledge

West Midlands Police (nd) 'Data driven insight & data science capability for UK law enforcement', available at http://www.excellenceinpolicing.org.uk/wp-content/uploads/2017/10/EIP17_2-5_Utilising_Data_Science.pdf (last visited 12 April 2019)

Wodinsky S 'Palmer Luckey's border control tech has already caught dozens of people' *The Verge* (2018), available at <https://www.theverge.com/2018/6/11/17448552/border-control-tech-security-lattice-palmer-luckey> (last visited 12 April 2019)

Wood M 'Some quick thoughts on the public discussion regarding facial recognition and Amazon Rekognition this past week' *AWS Amazon Machine Learning Blog* 1 June 2018, available at <https://aws.amazon.com/de/blogs/machine-learning/some-quick-thoughts-on-the-public-discussion-regarding-facial-recognition-and-amazon-rekognition-this-past-week/> (last visited 18 April 2019)

Online assemblies between freedom and order: Practices in South-East Europe

Andrea Jovanović, Edo Kanlić,** David Savić,*** Goran Stanić,**** and Kristina Ćendić*****†*

Abstract: This article approaches the question of whose interests the internet serves through the prism of online assemblies in the South-East Europe (SEE) region. In order to answer this question, the article uses four connected yet different angles. The first part explores opportunities and limitations of international laws, as well as national laws in the SEE region. Furthermore, the article discusses the role of the state in providing and facilitating access to the internet, that is, enabling the space for online assemblies in the SEE region. The article takes into account the variety of actors in the field of freedom of expression and freedom of assembly online, paying special attention to internet service providers. Finally, the article analyses the surveillance of the internet activities and security and its relation with online and offline assemblies. The article uses all four these aspects to explore the situations in the SEE region. The article specifically focuses on four countries, namely, three former Yugoslav republics: Croatia – a European Union member since 2013; Serbia – a candidate country exercising control over the internet the most; Bosnia and Herzegovina – a country aspiring to become a candidate but in which progress is burdened by divisions and legacy of the war; and Turkey, which has one of the most illustrative examples of stifling freedom of expression and assembly, and the influence of which on the Balkans is also visible.

Key words: online assemblies; South-East Europe; freedom of assembly; freedom of expression

1 Introduction

Freedom of expression is one of the pillars of democracy and therefore it is important to emphasise a high level of interplay between this right and other human rights. Freedom of expression not only is a constitutive right, but also an instrumental one, which is why its 'interaction with a number of other rights vouchsafed by international human rights law is notably dynamic' and it 'generates enhanced understandings and applications of the rights in question' (McGonagle 2011). 'The suggested

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. BA (Philosophy); aerdna.1112@gmail.com

** MA (Democracy and Human Rights); edo.kanlic@gmail.com

*** MA (Democracy and Human Rights); david.savic@live.com

**** MA (Democracy and Human Rights, Theology and Religion); gost93@gmail.com

***** PhD (Communication Studies); kristina.cendic@gmail.com

† We wish to extend a special acknowledgment to Nina Belyaeva – Professor, Department Head; National Research University "Higher School of Economics" (HSE); nbelyaeva@hse.ru

principle that the government can simply ignore rights to speak when life and property are in question so long as the impact of speech on these other rights remains speculative and marginal it must look elsewhere for levers to pull.' The article explores the interaction between the right to freedom of expression and the right to assembly in South-East Europe and focuses on the online sphere and the exercise of the two rights on the internet.

The article approaches the question of whose interests the internet serves through the prism of online assemblies in the South-East Europe (SEE) region. In order to answer this question, the article uses four connected yet different angles. The first part explores opportunities and limitations of international laws, as well as national laws in the SEE region. Furthermore, the article discusses the role of the state in providing and facilitating access to the internet, that is, enabling the space for online assemblies in the SEE region. The article takes into account the variety of actors in the field of freedom of expression and freedom of assembly online, paying special attention to internet service providers. Finally, the article analyses the surveillance of the internet activities and security and its relation with online and offline assemblies. The article uses all four these aspects to explore the situations in the SEE region. The article specifically focuses on four countries, namely, three former Yugoslav republics: Croatia – a European Union (EU) member since 2013; Serbia – a candidate country exercising control over the internet the most; Bosnia and Herzegovina – a country aspiring to become a candidate but in which progress is burdened by divisions and legacy of the war; and Turkey, which has one of the most illustrative examples of stifling freedom of expression and assembly, and the influence of which on the Balkans is also visible.

2 Theoretical and legal considerations related to online assemblies and freedom of expression

2.1 The level of recognition of 'online rights'

If the policy makers were to define the right to an online assembly under the Universal Declaration of Human Rights (Universal Declaration 1948), they would have to face rigorous precision requirements set by Eleanor Roosevelt (Fazzi 2017). In addition, under article 31 of Vienna Convention on Law of Treaties (VCLT 1980), the context and the meaning of any international treaty has to be understood in a very clear context by the parties, when it comes to the implementation and interpretation of the Treaty (VCLT 1980). As of now, there is no clear definition on what exactly the right to an online assembly is in legal or social context. Therefore, we must ask how we define the right to an online assembly and the position of the citizens towards this right, and what the role played by the state would be in such predicament. In order to answer this question, this article will define the right to an online assembly by combining the already-existing theoretical and legal frameworks. Under such conditions, the hypothesis is that the internet could be approached as a form of a virtual public space, which allows groups of people to freely express their ideas and opinions, and to be able to form an assembly within the virtual public space.

In the book *Negotiating digital citizenship*¹ the authors define the internet as an epoch which has the potential to create a new form of relation between the citizens and the states (McCosker, Vivienne & Johns 2016). However, this relationship of the internet has to be 'characterised by openness, sharedness and free exchange' (McCosker, Vivienne & Johns 2016). Such characterisation of the internet very closely resembles the guarantee of the right to freedom of opinion and expression, which has been enshrined in article 19 of the Universal Declaration (1948). In order to exercise these rights, the citizens may 'receive and impart information and ideas through any media and regardless of frontiers' (Universal Declaration 1948). The internet may be seen as a platform which disseminates information and ideas, while it disregards obstacles of national borders. The European Convention on Human Rights (European Convention) safeguards freedom of expression in its article 10. In addition, the European Court and European Commission of Human Rights described freedom of expression as 'one of the basic conditions for the progress of democratic societies and for the development of each individual'. The European Court gives a wide interpretation to article 10, and one of the landmark statements is found in the case of *Handyside v United Kingdom*¹ where the Court said that the scope of freedom of expression is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also those that offend, shock or disturb the state or any sector of the population.² What is clear from *Handyside v United Kingdom* is that it is expected of states to give the broadest possible interpretation to freedom of expression, in the interests of promoting democratic values. The Court has interpreted freedom of expression to cover all forms of expression and it extends to all forms of opinions and views, approaching the restrictions of freedom of expression given in article 10(2) only in exceptional cases.

In order to engage in the public debate in which the citizens can freely express their ideas and opinions, a form of public space has to be provided. Habermas in his book *The structural transformation of the public sphere* has coined a term 'the public sphere,' by which he defines a zone where free discussion between the citizens and the state may take place (Habermas 1991). The setting of the public sphere is crucial for a modern and democratic society, as such practice serves the citizens to publicly criticise the state and, by doing so, to shape a narrative which is closely related to the citizens (Habermas 1991). Additionally, an open discussion within the public sphere 'refers to an attitude toward social cooperation, that of openness to persuasion by reasons referring to the claims of others as well as one's own' (Habermas 2003). Following the Habermasian line of thought, the internet may be seen as a form of the virtual public sphere, as social media, blogs and other types of forums allowed the citizens to freely and publicly express their views online, where their voices can be seen. The United Nations (UN) 2030 Agenda for Sustainable Development also recognises that the 'spread of information and communications technology and global interconnectedness has great potential to accelerate human progress' (Sustainable Development 2018). Therefore, through the internet

1 *Handyside v United Kingdom* App 5493/72 ECHR, 7 December 1976 para 49.

2 Freedom of Expression Under the European Convention on Human Rights article 10, Interights manual for lawyers, current as at October 2009.

citizens and states can collaborate together and benefit from open discussion, which should create modern democratic societies.

The crucial element to an open discussion are the citizens. Their voices are part of the productive and civil practice, which allows their participation that may be exercised online (McCosker, Vivienne & Johns 2016). However, the participation usually coincides with the action of particular groups of citizens. In the real world, the groups of citizens often opt for the creation of assembly, which is their guaranteed right according to article 20 of the Universal Declaration. The assembly may be defined as a 'temporary presence of a number of individuals in a public place for a common expressive purpose' (OSCE/ODIHR 2010). This particular definition of assembly may easily be transferred to an online public sphere. The participation and the expressive purpose of an assembly is far easier to be created online today than it is in the real world. The citizens, at least in the developed parts of the world, have an unprecedented access to a public sphere such as the internet, where they can interconnect extremely fast with other individuals or groups. Such connectivity would allow real-time interventions and innovative forms of collaboration (Soh, Connolly & Nam 2018).

Therefore, we may conclude that the right to online assembly should be finally defined, as a guaranteed right to form an assembly in any form or shape on the internet, which is a form of virtual public space. Such civil practice would allow citizens to freely participate and express their purposes and opinions, with the minimum intervention by the state or any other actor. However, the main aspect of an online assembly has to be focused on the peacefulness and the safety of assemblies, which should be a positive obligation that requires public authorities to take action. What is necessary to discuss further in depth is the role of the state and the role of the private sector, which in this case would be the owners of internet service providers. As the right to online assembly is not defined by the international legal system, there currently is a lot of space for ambiguity and uncertainty. This is especially problematic nowadays, since states and the private sector are starting to exert increasing control over the online spaces, under the excuse that they are obliged to provide peace and safety for internet users, hence the citizens. In the next few chapters we will examine to what extent states and internet service providers are primarily ensuring the safety of their citizens, or whether they are overstepping their boundaries by exerting excessive control, which may be harmful for freedom of expression and democratic values.

2.2 The role of the state to provide/facilitate internet access

Among obligations that nation states have as core actors in international politics, they also play a crucial role in providing and facilitating access to the internet for their nationals. Answers to the question of how much states should be involved in facilitating and regulating internet access vary from Hobbes's controlling monster state to Bakunin's vision of collectivist anarchy (Herold 2008). There are those who see the internet as the last truly free place, while some see it as a lawless sphere. Governments of developed states have been focused largely on creating the conceptualised international settings of the internet. States' obligations regarding the internet were mainly agreed and defined through international organisations, with the UN bodies who were pioneers in that field.

In order to understand the process of states' involvement in providing and facilitating internet access, it is necessary to overview the role that the internet plays regarding the implementation of some human rights. The UN Human Rights Committee (UNHRC) has called on states to ensure access of individuals and to foster the independence of the internet, which is interpreted as a new trend in technologies (General Comment 34 Article 19: Freedoms of opinion and expression 2011) through which freedom of opinion and expression (Universal Declaration 1948) can be implemented without interference. According to the Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, the internet is seen as an 'enabler' or catalyst for individuals to exercise their rights, such as the right to education of the right to take part in cultural life, as well as the rights to freedom of association and assembly (La Rue 2011). According to all relevant documents regarding the internet, all the rights individuals have offline must also be protected online, in particular freedom of expression.

Investing in information and communication technologies is one of the Sustainable Development Goals accepted by the all member states of the UN and the internet is perceived as a booster of economy and development of individuals and states (Blazhevska 2017). However, having well-being as one of the significant factors that determines who can access information communications technologies, the internet is likely to be concentrated among socio-economic elites in countries where internet penetration is low (La Rue 2011). This means that by providing and facilitating internet access, states should have in mind the costs this produces, therefore becoming an obstacle in broader internet consumption.

When examining states' approaches in providing and facilitating internet, before the mid-2000s policy makers were mostly focused on infrastructure, and by that time at least 70 per cent of the world's population lived within the range of a mobile internet signal, which makes that process successful (Internet Access for All 2016). Internet Society, an American non-profit organisation founded to provide an organisational home and financial support for the internet standards process, provides policy principles for expanding access infrastructure. Some of the most important principles are the removal of barriers to investment and competition; the creation of transparent and affordable licensing processes; collaboration with neighbouring governments in order to harmonise and coordinate regional cross-border interconnection and licensing regimes; and avoiding burdensome taxes on end-user services (Internet Access for All 2016).

The role of states in providing and facilitating internet access also includes the usage of their power concerning possible restrictions in that field. In the era of globalised fear and securitisation of politics, nation states use national laws to interpret restrictions on the internet more strictly than is the case with rather vague international norms. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) states that everyone has the right to hold opinions without interference and the right to freedom of expression (OHCHR International Covenant on Civil and Political Rights 1966). Nevertheless, this article recognises certain restrictions regarding freedom of expression, which should be provided by law and are necessary for respect for the rights or reputations of others; for the protection of national security, public order, public health or morals.

These provisions gave an open door to states to interpret given exceptions in different ways through their national laws, including cutting off access to the internet entirely. The UN Special Rapporteur considers this practice disproportionate and a violation of article 19, regardless of the justification provided, including times of political unrest or even war (La Rue 2011). Practice in the states of South-East Europe shows how these states are mostly focused on control of the internet, through various forms of restrictions, rather than on infrastructure that is on a very low level compared to the other regions in Europe. This issue will be discussed more in detail in the next part.

2.3 Online as a 'space for assembly'

From the very beginning the internet was regarded as a free and inclusive space with the intention of becoming available to everyone. The period of the 1960s to the 1980s was marked by a collective spirit shared by computer scientists, professionals and others involved in the internet development. They saw it as a communal space for an 'open and non-hierarchical' culture. On the other hand, the internet also had a very anti-commercial character. This changed during the 1990s when, in the words of McChesney, the internet was transformed from a public to a 'capitalist sector' (McChesney 2013). Formally privatising the internet left it open to mysterious and non-transparent market forces, and its goals and course changed accordingly. While this process was secret and mostly 'behind the curtains',³ it had a significant impact on the way in which online space has been further conceived as 'public' and 'private'.

Market and commercialisation changed the situation and internet service providers started to influence laws and legislation. One of the most important 'battles' has been over Net neutrality, a principle that causes internet service providers to treat all communications on the internet equally and to 'not discriminate or charge differently based on user, content, website, platform, application, type of equipment, or method of communication' (Gilroy 2011). Profit-driven internet service provider companies have an obvious financial interest in abolishing this principle, but the consequences in many countries can be rather political if 'a small handful of private concerns have a censor's power over what had become the primary marketplace of ideas' (McChesney 2013). The dangers are numerous: the pricing of the services, censorship, privacy issues and, finally, surveillance.⁴ The issues regarding internet service providers are mainly assessed on a case-to-case basis. An important case is *Delfi v Estonia* which refers to whether there was an active role of the website when it comes to enabling third-party comments. In this case, the European Court of Human Rights 'acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitute an effective remedy for violations of personality rights'. On the other hand, the Grand Chamber stated that 'Delfi cannot be said to have wholly neglected its duty to avoid

3 McChesney asserts that 'the media watch group Project Censored ranked the privatization of the Internet as the fourth most censored story of 1995' (McChesney 2013).

4 These problems so far are much more visible in non-Western parts of the world, such as China and sub-Saharan Africa (Skycoin 2018).

causing harm to third parties, but the automatic word-based filter failed to select and remove odious hate speech and speech inciting violence posted by readers and thus limited its ability to expeditiously remove the offending comments'. Another case before the European Court of Human Rights which referred to intermediary liability is *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*. The Court stated that the applicants 'could foresee, to a reasonable degree, the consequences of their activities under the domestic laws. In doing so, the Court placed considerable emphasis on the fact that the Applicants were a self-regulatory body and a media publisher running 'a large internet news portal for an economic purpose.'

Overall, what changed in the exercise of the human right to freedom of expression is the number of platforms for this exercise because 'the internet has now become one of the principal means of exercising the right to freedom of expression and information'. Accordingly, the number of actors that may be liable for problematic content also increased. However, it is not necessary to introduce new, stricter provisions related to the internet, but more attention is needed when balancing freedom of expression exercised online and, for example, the rights of others (McChesney 2013).

On the other hand, the idea of transferring 'offline' rights to 'online sphere' described before has become much more vague than in the era of collective internet optimism during the 1960s and 1970s. Since most of the important human rights protection documents were written during the non-internet or early internet phase, its direct transmittance to a very specific internet field became impossible. That is one of the reasons why the Internet Rights and Principles (IRPC) Dynamic Coalition in 2010 developed the IRCP Charter and released it at UN Internet Governance Forum (IGF) in Vilnius, Lithuania. In this document, Article 7 – Freedom of Online Assembly and Association – translates article 20 of the Universal Declaration (Universal Declaration of Human Rights 1948) to online space in the following manner: 'Everyone has the right to form, join, meet or visit the website or network of an assembly, group or association for any reason. Access to assemblies and associations using ICTs must not be blocked or filtered' (IRCP Charter 2018). However, this is only part (a) of the article. The rest is still being drafted and may have a significant impact on how the conception of online space as a space for assembly will develop, especially combined with other rights provided for by this Charter. There are many perspectives to this and when all factors are taken into account, the opportunities and dangers occasioned by online space become more complicated.

2.4 Surveillance and security

After an examination of the providers and the very nature of the internet space itself, it remains critical to focus on the status and examples of protective measures and the possible abuses of the web environment. Surveillance and security on the internet define the relationship between online *freedom* and *order*, comprising both legislative and ethical practices that overlap respectively. Moreover, the relevance of the privacy of web users has become even more focal during the last decades since cyber threats are estimated by world governments and security organisations as global danger number one, thus replacing terrorism as the number one

global threat (Contreras et al 2013). In fact, one might claim that terrorism significantly generated the increase of protective measures that can further be abused for surveillance practices. Perry and Roda (2017) claim that

with the advent of terrorist attacks worldwide, many governments have pushed through legislation permitting online surveillance policies that may violate international treaty commitments and domestic law, particularly with respect to due process and legal consent. Electronic surveillance is a controversial form of data compilation because it is by nature virtual, leaving no physical trace to the untrained eye.

The ambiguity of online security described can most clearly be seen in the fact that the guarantees of privacy protection can never be clearly defined. Web security and privacy depend both on the fragile technological factors and on the users' online habits. It follows that 'a digital system that is not secured cannot be regarded as private, while having secured privacy of the system does not guarantee it is fully secured' (SHARE Foundation 2015).

Hence, it remains crucial to explore the question of how surveillance of our internet-based activities and the security thereof relate to freedom of expression characteristic to assemblies based both offline and online. Related to the topic of providers of internet access, a legitimate question to be asked is that if someone is to ensure protection and security, whether that does not cause the internet to be supervised by someone. Finally, is surveillance a *modus operandi* of online security?

The Guidelines on Freedom of Peaceful Assemblies drafted by the Organisation for Security and Co-operation in Europe (OSCE) state that '[a]ll types of peaceful assembly – both static and moving assemblies, as well as those that take place on publicly or privately owned premises or in enclosed structures – deserve protection' (Belyaeva et al 2010). Since the official instruction to protect online assemblies is still in the drafting process (also by the OSCE panel of experts) the presumption is that online assemblies deserve the same treatment. Yet, exercising protection does not exclude the possibility of interference in the private life, guaranteed by article 8 of the European Convention of Human Rights on privacy, if the actions of an individual or a group threaten national security or the freedom of others (Council of Europe 1953).

The experiences show that surveillance, under the guise of providing protection, not only interferes with privacy, but indeed can lead to severe censorship practices. This is evident from the fact that

electronic surveillance as currently practised by most states encroaches upon an individual's sacrosanct right to privacy, a fundamental right enshrined in Article 17 of the International Covenant on Civil and Political Rights. In many instances, electronic surveillance is a prelude to censorship. State censorship which involves the suppression of proscribed content and eventual sanctions against the user, is the next step in the digital surveillance chain (Perry and Roda 2017).

3 Online assemblies and freedom of expression in South-East Europe

When the internet arrived in Yugoslavia in 1991, it only connected three faculties of Belgrade University: the Faculties of Mathematics, Electro-

Technics and Political Science (RCUB). The network has spread further to other universities in Zagreb, Ljubljana and Novi Sad. Later on, the war in Yugoslavia slowed down the development and access to internet services. However, in 1992, in the midst of the war in Croatia, a group of human rights activists and students from Belgrade and Zagreb (and later also from Sarajevo) managed to go online, thanks to Open Society Funds and several other anti-war activists from Germany and The Netherlands. Together, they formed a platform called Zamir.net (in Serbo-Croatian at the time 'For Peace'), which was a platform that promoted anti-war efforts and other progressive ideas such as Lesbian, Gay, Bisexual, Transgender, Intersex and Questioning (LGBTIQ) rights and environmentalism. Zamir.net mainly assisted people to connect with their families in other countries, and to make sure that their family members survived attacks or were able to escape the war zones (Gessen 1995). This historic example in South-East Europe illustrates that the online assembly was formed out of the necessity for peace.

3.1 Bosnia and Herzegovina

Due to a very complex constitutional and administrative order in Bosnia and Herzegovina⁵ (BiH) it is very difficult to obtain unified data about internet penetration. The most recent data is from the Communications Regulatory Agency (RAK). This agency has published its report of the annual survey of users allowed to provide internet services in BiH in 2018. According to the report, by the end of 2018 there were 67 internet providers in the territory of BiH, with a total internet usage rate of 90,49 per cent (RAK 2019). The data provided in the report shows that the use of the internet in Bosnia and Herzegovina is on a steady pace and the agency expects that further liberalisation of the telecommunications market and the introduction of new technologies will enable the presence of quality services (RAK 2019).

On the other hand, state regulations regarding the internet are not as positive as the usage rate. When the Entity of Republika Srpska (RS) passed the Law on Public Peace and Order in 2015, it caused much controversy among the public. The president of the Entity stated that no limitations were placed on freedom of speech in this Entity but neither should any form of communication be misused (Halilović 2015). Among the public in BiH it is indisputable that hate speech, paedophilia and similar criminal activities are condemned, but with this law there are no restrictions on the ability of the state to regulate social networks and regular citizens expressing themselves. This is why the general impression among the Bosnian public is that the law was passed in order to keep an eye on all those who criticise the government (Halilović 2015). These obstacles are reflected first in the very adoption of necessary legislation that is affected by political pressures, just as it is the case with the content

5 The current political system in Bosnia and Herzegovina is the product of the Dayton Peace Agreement (1995). This Agreement stopped the brutal war which occurred after this state had proclaimed independence from the Socialist Federative Republic of Yugoslavia. According to Annex 4 (the Constitution of Bosnia and Herzegovina) of the Peace Agreement, Bosnia and Herzegovina has two entities and one district: Entity of the Federation of Bosnia and Herzegovina (mostly populated by Bosniaks and Croats) and Entity of Republika Srpska (mostly populated by Serbs) and District of Brčko.

of most media outlets (even public service programming), as they cannot be said to be independent to a great extent.

Specifically, when it comes to the RS's Law on Public Peace and Order, it is particularly worrying to include social media within the definition of a 'public space'. While such legislation is familiar to Western states, such as the United Kingdom, the interpretation of this legal trend is deeply concerning: It gives power to the police and magistrates and judges to interpret the law and sanction any social media action as they see fit. This is problematic, as the law does not include concrete standards for the definition of social media, nor does it explain what constitutes 'offensive' or 'indecent' material, nor denies that citizens can be prosecuted outside of RS. Democratic societies should be void of such arbitrary provisions as they violate the freedom of expression of internet users, which has been commonly recognised under international law (European Convention on Human Rights 1950; OHCHR International Covenant on Civil and Political Rights 1966; Universal Declaration of Human Rights 1948).

The government must be able to 'establish that the expression poses a serious threat to national security' and the restriction constitutes the 'least restrictive means' available. 'Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know' (Johannesburg Principles on National Security 1996).

The government does not state any explicit reason for detaining the users of social networks. Furthermore, there is no proven causal link between any incidence of violence and posts on social networks. Such a link must be established first in order for the aim of protecting the public order to be viable (Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights 1984).

The contents of the posts on social networks because of which the authors were detained do not intend or seem likely to incite riot or any threat to national security, and there is no proof, only a speculative link between the posts and possible threats to public order. One of the most important cases in this connection was that of a journalist, Danijel Senkić, also a representative of an NGO 'front'. On his Facebook wall, Senkić spoke about the authorities in BiH when they arrested Bosniak returnees in RS, and called their activities acts of terror, and described some police officers as 'criminals' and Bosniak politicians as 'mute observers' (Senkić 2015). Interesting is the fact that Senkić was detained despite the fact that he lives in a part of BiH that is out of the reach of the disputable law mentioned above (Dodikova diktatura i u FBiH 2015). At the same time, the authorities did not focus on the verification of information regarding war crimes, but on prosecuting a person who speaks on their Facebook wall. Experts agree that the only way in which it would have been possible for Danijel Senkić to come before court would be for defamation, and only if he would be the person accused of committing the crime (Halilović 2015b).

The most recent case concerning the role of the state and internet restrictions in BiH occurred in April 2019. Good cooperation between the portal Klix.ba, state institutions and internet providers resulted in the arrest of three people in the territory of BiH in only five days, for writing

hate speech in comments on the news portal Klix.ba (Za pet dana u BiH uhapšene tri osobe zbog govora mržnje na internetu 2019). The portal warns about online hate speech as the crucial problem on the internet and calls for citizens/users to report it.

3.2 Serbia

It is a fact that in recent times internet users have succeeded in finding ways to avoid restrictions. However, it is clear that the physical infrastructure in the territory of a particular country cannot, at least legally, exist without the permission and consent of state authorities (Perkov 2017). The most thorough regulation in Serbia is the Electronic Communications Law. Apart from this, electronic surveillance is especially regulated by the Code of Criminal Procedure, the Law on the Military Security Agency and the Military Intelligence Agency, as well as the Law on the Security and Information Agency. All these regulations oblige operators to set up their network infrastructure in a certain way, in order to provide the ability to intercept communications and retain communications data (Perkov 2017).

The field that is the most problematic for Serbian authorities includes social networks. Media and experts close to the Serbian President often use the example of Turkey when justifying control over the internet. Under Erdogan, there is constant control over the messages sent through social networks in Turkey, and one cannot write what one wants or criticise him. In Serbia, an environment prevails in which insults and defamations are exchanged at will (Kurjački 2017).

This is the example of how an analyst, Vuk Stanković, commented on a situation regarding the programming of the pro-government Pink TV Channel. This channel has a national frequency and has a great influence on public opinion. On the other hand, Nedim Sejdinović from the Independent Journalists Association of Vojvodina sees this statement as an open call for internet regulation, which would open up an enormous space for abuse in terms of 'banning' certain content that does not suit authorities (Kurjački 2017).

If the state intends to punish the owner or author of the platform for violating domestic regulations, such a possibility exists if the head office or representative office is located in its territory (Perkov 2017). Nevertheless, out of the 100 sites most visited, 60 per cent of sites do not have any connection with Serbia, which means that the platforms most commonly used by citizens of Serbia are wholly beyond the reach of the state (Perkov 2017).

When it comes to using the platforms for assembly, an ongoing massive weekend protest in the capital Belgrade, '#1od5miliona', mobilised through online platforms after a murder and violent attacks on politicians from the opposition, can serve as an example. Professor Đorđe Krivokapić claims that the internet is the only media platform in Serbia that can generate significant critique and mobilisation of citizens since other media is controlled by the state (Čilić 2019).

Another danger to the online sphere in Serbia is presented by the recent installation of closed-circuit television in Belgrade. Since video surveillance in public spaces is not regulated in Serbia, it remains

controversial to what degree personal privacy is protected knowing that surveillance cameras have an option of facial recognition (SHARE Foundation 2019). Moreover, similarly to the case of Croatian disclosure of personal data of insolvent persons, the numerous examples of hacking attacks in Serbia display how insecure online platforms of both governmental institutions and NGOs are. Although Serbia has an Emergency Response Team (CERT) that coordinates prevention and protection from security risks in ICT systems on the national level, (Trusted Introducer: Directory: SRB-CERT nd), the hackers' attacks remain frequent. For instance, in 2018 four centres for social work across the country were hacked in order to collect personal data of the victims of violence (FoNet 2018). The Chamber for Public Sales was also hacked, disabling the visibility of more than 20 000 public offers (021 2018). In the same year, the email addresses of the Office for Refugees and Migration were hacked and used to send messages to different recipients (DD 2018).

3.3 Turkey

The examples of Turkey under the current President Erdogan, a country not only with a historical-cultural influence on the SEE region that started with the expansion of the Ottoman empire in the fifteenth century, but also with a strong current political and economic influence on Bosnia and Herzegovina and other countries, are instructive in scrutinising practices of surveillance of the online assemblies. Followed by the 2016 *coup* attempt against the government of Erdogan's AKP (Justice and Development Party), many internet platforms and internet service providers in general faced severe surveillance and controlling strategies exercised by the government. The group of Turkish scholars examined the post-*coup* internet policies in the country and offered their key findings (Yesil et al 2017):

The AKP's post-*coup* strategies concerning the internet are culminating in a distributed network of government and non-government actors using hard and soft forms of control. While the AKP continues to deploy existing internet law, anti-terror law and press law provisions and further expands its online hegemony by way of decree laws, its post-*coup* internet policy has also come to rely on the opaque activities of users and groups who are affiliated with government officials, party members and partisan media outlets and whose primary objective is to target and harass government critics on social media, and intimidate those who dissent.

As a consequence, in 2018 Freedom House described internet freedom in Turkey as severely manipulated by the government, which was frequently removing or blocking internet content, and because of which it was given 'non-free' internet status (Freedom House 2018).

3.4 Croatia

In Croatia, the youngest EU member and the second of former Yugoslav countries after Slovenia, two phenomena related to online assemblies and democracy dynamics can be observed. The first is the rise of populist parties, notably *Živi zid* (Human shield), which arose after online-supported anti-government protests. The so-called 'Facebook protests' in 2008 effectively marked the beginning of online-supported protests in Croatia. However, since more than 60 000 people confirmed their attendance, whereas only a few thousand people gathered in the capital

Zagreb, media characterised the Croats as rebels only on the internet and rightly pointed out that protests initiated on Facebook had failed (Werman 2008; Valich 2008). Yet despite the failure, the leader of the protest, Ivan Pernar, and his populist party *Živi zid* has increasingly become one of the most relevant political actors in the country ten years later. Their main political activity is the fight against foreclosure methods and enforced evictions with which banks deprive indebted individuals and families from their houses. Besides organising resistance towards police officers in front of the confiscated houses, they became popular also because of their strong anti-EU stance and because of the promotion, using their social media profiles, of bizarre conspiracy theories such as urging people not to vaccinate their children since, according to them and other promoters of this theory, this can cause autism and similar conditions (NACIONAL 2017).

A related phenomenon of the SEE region, namely, the foreclosure trend manifested in the myriad of executed bankruptcies, is an example of weak legal protection of personal data. With a population of around four and a half million, Croatia has more than 300 000 people/families in foreclosure status, mostly due to falling into debt using Swiss currency of which the value significantly decreased in the 2010s. Since 2013 people hit with foreclosure measures are gathered in the association *Blokirani* (*Blokirani.hr* nd). However, in the beginning of 2019 the courts were allowed to publish personal information of the bankrupted individuals and thus increase their public visibility and consequently personal and financial vulnerability. The personal data of more than 100 000 people was made public, but the Ministry of Justice claims that the right to privacy is not violated since the courts are supposed to work transparently (N1 2019).

4 Conclusion

Our research demonstrated that the internet serves different interests in the SEE region. Although one notices an increase in the online mobilisation of public protests, the interest primarily remains in the hands of the governments to exercise control and in the hands of the state-owned companies to maintain monopoly through providing their services. Further, it is important to underline that the progress in the understanding and use of the internet for civil purposes is still burdened by divisions, the legacy of the war and transition in the countries of the SEE region. Thus, rather than exercising and promoting social rights, online platforms are predominantly used by 'troll armies' to spread hatred speech based on national, ethnic, religious, political and other differences. In the context of the global scene, we noticed that regional legislation does not follow technological progress, resulting in the weakly-developed legal system of protection that is always slow to follow the increasingly fast development of new virtual instruments.

First, the article provided a detailed overview of the theory and international human rights law, in order to offer a setting in which the enjoyment of the two rights occurs. The most relevant for the region in this respect is the European Convention on Human Rights and Fundamental Freedoms (European Convention) and the practice of the European Court of Human Rights. Article 10 of the European Convention

safeguards freedom of expression in its first sub-section, and explains limitations to the exercise of this right in sub-section 2. Article 11 refers to the right to assembly, the restrictions of which are similar to the mentioned restrictions in article 10: the interests of national security or public safety; the prevention of disorder or crime; the protection of health or morals; and the protection of the rights and freedoms of others.

The article further explored the role of the state to provide or facilitate internet access. It has been acknowledged that the internet is not a specific platform which requires more regulation, which is why some actions taken by states in the region have been assessed as rather questionable. This article sifts through various examples of advantages and disadvantages regarding internet regulation, but emphasises that the UN Human Rights Committee urged states to ensure internet access to individuals, maintain its independence and its possibilities of providing more space for exercising human rights. Moreover, the fact that the internet is gaining momentum also brought numerous new actors into play, which is why the article is specifically directed at explaining the role of internet service providers, drawing the line between active and passive actors and highlighting the level of editorial liability in this respect.

The article acknowledges the dehumanisation, internationalisation and privatisation of the internet by pointing to the fact that internet service providers have a substantial influence on all aspects of the online sphere and indirectly also on new regulations. The question of net neutrality has attracted specific attention as it causes internet service providers to treat all communications on the internet in the same manner regardless of the type of communication used. The article agrees that profit-driven internet service provider companies have a certain financial interest which may present problems in terms of censorship, privacy issues, the price of the service as well as fake news. Platforms, advertising agencies, advertising networks and the networks and service providers that provide internet access to consumers benefit because they depend on consumers spending more time with a certain type of content and they track profiles of consumers, thus providing them with the content they identified as relevant for certain users.

As far as the interdependent nature of freedom of expression and freedom of assembly is concerned, the article introduces the topic of surveillance and security. The article perceives surveillance mainly as a tool of states to exercise control over the internet and explores the interplay between the two rights, in addition to the right to privacy enshrined in article 8 of the European Convention. The relevance of privacy of web users is an issue that is gaining momentum as cyber security has in the past few years often been in jeopardy. Web security and privacy depend both on technological factors and on the users' online habits. However, as they are easily tracked down, the article acknowledges that there is no guarantee to provide users with full protection, because their activities online are easily visible to network providers, advertisers and even state authorities, and because users often are unaware of the fact that in addition to their rights to be online, they also have responsibilities.

When it comes to legal restrictions placed on freedom of expression and freedom of assembly in the region of South-East Europe, one of the most recent examples is the Law on Public Peace and Order adopted in Republika Srpska – one of the two entities of Bosnia and Herzegovina. The

most problematic aspect of the law is, the lack of the definition of public space. According to local and international experts, the reason for assessing this law to be restrictive lies in its application, because on several occasions public space included social networks and their users were detained by the police. Just as in most examples referring to Bosnia and Herzegovina, the posts dealt with war and war crimes, but there was no sufficient basis to claim that their posts intended or were likely to incite riot or any threat to national security, that is, to public order. In this manner, the authorities not only exercised their control over the online sphere, but they also caused a chilling effect among social network users and made the scope of the restrictions questionable, by detaining persons who were not based in the territory of Republika Srpska, but in the Federation of Bosnia and Herzegovina, the other entity in BiH.

On the other hand, Serbia has seen a rapid decrease in freedom of expression in the past few years, because the state aims at penetrating the online sphere in terms of restrictions and monopoly over internet service providers. In Serbia only two companies provide internet services, namely, Telekom Serbia and SBB. Of these almost 80 per cent of the population uses the former connection, Telekom Serbia, owned by the state. The article explains that there is a panoply of laws referring to the online sphere: the Electronic Communications Law; the Code of Criminal Procedure; the Law on the Military Security Agency and the Military Intelligence Agency; as well as the Law on the Security and Information Agency. All these regulations oblige operators to have their network infrastructure set in a specific manner. This makes the interception of communications and the tracking down of users easy and thus the users' data are rather susceptible to misuse. Now more than ever, the right to freedom of expression and the right to freedom of assembly go hand in hand in Serbia because social networks and online groups are largely used for protests that have for months been going on in Serbia. The article identified the occasions on which these rights were violated, and acknowledged the dangers of state authorities banning certain content, spreading fake news and directly pointed at the attacks experienced by some journalists and protest organisers. The deteriorating state of freedom of expression, freedom of assembly and right to privacy in Serbia is also illustrated by the recent installation of closed-circuit television in Belgrade and the numerous examples of hacking attacks in Serbia. It is particularly disturbing that surveillance in public spaces is not regulated in Serbia, and as protests are occurring and cameras are installed, it is not known to what extent and for which purpose the facial recognition option with cameras will be used by the authorities.

Furthermore, the article discussed trends in Turkey which exercised substantial control over online assemblies. In 2016 Turkey saw an attempt at a *coup d'état* and many internet platforms, internet service providers and even 150 media experienced shut-downs and extremely strict surveillance and controlling strategies exercised by the government. This event has changed internet policies in Turkey as the government used hard and soft forms of control to a great extent all over the internet. The article also acknowledged the fact that the right to freedom of expression and the right to peaceful assembly have been casualties of internet law, anti-terror law and press law. Academics were detained when mentioning problems in the country on conferences; journalists and activists were detained due to their actions taken against the regime that oppressed basic human liberties;

authorities were denied permission to attend traditional May Day demonstrations in Istanbul; and so forth. The rights to online assembly and freedom of expression were violated with every denial of internet access during security operations, several news and citizen journalism websites were blocked, and even Wikipedia was inaccessible while most users of social networks such as Twitter and Facebook received numerous requests for content removal. The article clearly identified the problems faced by online users and pointed at censorship and a substantial level of control over internet by the authorities, which not only jeopardised their exercise of human rights, but often altogether disabled their exercise in the online sphere.

The article finally explored the current state of online assembly and freedom of expression in Croatia. As a new EU member, Croatia had to make its legislation compliant with the EU accession requirements and it has not seen serious cases of censorship or shut-downs. The activities on social networks in Croatia were, on certain occasions, precisely that – the activities on social networks only. Therefore, even though there were initiatives to mobilise protesters via the online sphere, in the offline sphere not many persons were very active. On the other hand, Croatia has seen a rather serious example of privacy violation and the misuse of data gathered through an online group. After executed bankruptcies performed by the banks, the courts were allowed to publish the personal data of over 100 000 bankrupted individuals gathered around the association Blokirani. In this manner the authorities exploited the members of the group and their data which may have had a chilling effect, because it would mean that people cannot freely join groups and thus share similar problems and work for the same cause either in the online or offline sphere, if their personal information is in jeopardy when they do so.

By analysing the examples of countries in South-East Europe, the article explored the interaction between the right to freedom of expression and the right to peaceful assembly. It showed that in the online sphere, the two rights are tightly connected because the internet opened numerous opportunities of gathering people, mobilising through social networks and provided a new space for debates. This space has become increasingly active and vibrant, much activism in the region shifted from the offline to the online world, and this trend was also recognised by the authorities. Therefore, the internet policies in these countries have undergone vast changes, and legislative frameworks have been amended or interpreted rather broadly in order to be more applicable to the online sphere. It seems that such attempts have not thus far been very successful, because instead of enabling and protecting new ways of freedom of expression and of assembly, the states limited the access, caused chilling effects or censored the online content in order to exercise more control over the internet. 'One of the great paradoxes of democracy is that if it functions well, criticism of it will thrive' (McGonagle 2011). Therefore, if public participation, assembly and expression on the internet are thwarted either by legislation, blocking, filtering or causing a chilling effect, then democracy and the enjoyment of human rights in South-East Europe seem shaky and their future rather uncertain.

References

- A policy framework for enabling internet access (2016), available at <https://www.internetsociety.org/resources/doc/2016/a-policy-framework-for-enabling-internet-access/> (last visited 4 April 2019)
- Belyaeva N 'Organisation für Sicherheit und Zusammenarbeit in Europa' Office for Democratic Institutions and Human Rights, Europarat (eds) 2010. Guidelines on freedom of peaceful assembly. OSCE/ODIHR, Warsaw/Strasbourg
- Blazhevskaja V (2017) 'Sustainable Development Goal 9: Investing in ICT access and quality education to promote lasting peace', available at <https://www.un.org/sustainabledevelopment/blog/2017/06/sustainable-development-goal-9-investing-in-ict-access-and-quality-education-to-promote-lasting-peace/> (last visited 4 April 2019)
- Blokirani.hr nd Blokirani, available at <http://www.blokirani.hr/> (last visited 4 May 2019)
- Čilić U (2019) Krivokapić: Građanska pobuna na društvenim mrežama Radio Slobodna Evropa, available at <https://www.slobodnaevropa.org/a/srbija-protesti-mreze/29785214.html> (last visited 4 May 2019)
- Contreras JL, DeNardis L & Teplinsky M 'Mapping today's cybersecurity landscape' (2013) 62 *American University Law Review* 1113
- Dodikova diktatura i u FBiH: Tuzlak na saslušanju u policiji zbog statusa na FB (2015) Novinska Agencija Patria, available at <https://nap.ba/news/13080> (last visited 4 June 2019)
- Fazzi D 'Eleanor Roosevelt's peculiar pacifism: Activism, pragmatism, and political efficacy in interwar America' (2017) 12 *European Journal of American Studies: Special Issue – Eleanor Roosevelt and Diplomacy in the Public Interest*, available at <https://journals.openedition.org/ejas/11893> (last visited 28 April 2019)
- ForNet P (2018) Poverenik: Pokrenuti prekršajni postupci protiv nekoliko centara za socijalni rad Dnevni list Danas, available at <https://www.danas.rs/drustvo/poverenik-pokrenuti-prekršajni-postupci-protiv-nekoliko-centara-za-socijalni-rad/> (last visited 28 April 2019)
- Freedom House (2018) 'Turkey', available at <https://freedomhouse.org/report/freedom-net/2018/turkey> (last visited 28 April 2019)
- Gessen M (1995) Balkans Online Wired, available at <https://www.wired.com/1995/11/zamir/> (last visited 28 April 2019)
- Habermas J (1991) *The structural transformation of the public sphere: An inquiry into a category of bourgeois society* trans Burger T & Lawrence F Cambridge and Massachusetts: The MIT Press
- Habermas J (2003) *On the pragmatics of communication* Oxford: Blackwell Publishing Ltd
- Halilović M (2015) Veliki brat u vašoj kući. Analiziraj.ba., available at <https://analiziraj.ba/2015/02/11/veliki-brat-u-vasoj-kuci/> (last visited 4 April 2019)
- Halilović M (2015) PROGON GLASNIKA LOŠIH VIJESTI. Analiziraj.ba., available at <https://analiziraj.ba/2015/07/02/progon-glasnika-losih-vijesti/> (last visited 4 June 2019)
- Herold DK 'Development of a civic society online? Internet vigilantism and state control in Chinese cyberspace' (2008) 2 *Asia Journal of Global Studies* 26

- Kurjački N (2017) Da li bi moglo da dođe do cenzure društvenih mreža u Srbiji? N1 Srbija available at <http://rs.n1info.com/Vesti/a333532/Da-li-bi-moglo-da-dodje-do-cenzure-drustvenih-mreza-u-Srbiji.html> (last visited 4 April 2019)
- La Rue F (2011) 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development', available at https://doi.org/10.1163/2210-7975_HRD-9970-2016149 (last visited 4 April 2019)
- McCosker A, Vivienne S & Johns V (2016) *Negotiating digital citizenship: Control, contest and culture*. London and New York: Rowman & Littlefield International Ltd
- N1 (2019) Koliko su nam zaštićeni osobni podaci?, available at <http://hr.n1info.com/Vijesti/a369370/Koliko-su-nam-zasticeni-osobni-podaci.html> (last visited 4 May 2019)
- NACIONAL (2017) PERNAR 'U cjepivo su stavili nešto da nas trajno obilježi, žigoše ko stoku', available at <https://www.nacional.hr/pernar-u-cjepivo-su-stavili-nesto-da-nas-trajno-obiljezi-zigose-ko-stoku/> (last visited 28 April 2019)
- OHCHR International Covenant on Civil and Political Rights 1966, available at <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> (last visited 4 May 2019)
- OSCE and ODIHR (2010) *Guidelines on Freedom of Peaceful Assembly* Warsaw and Strasbourg: Organisation for Security and Co-operation and Office for Democratic Institutions and Human Rights (ODIHR), available at <https://www.osce.org/odihr/73405?download=true> (last visited 28 April 2019)
- Perkov B (2017) Nadležnost Srbije na internetu, available at <https://labs.rs/rs/nadleznost-srbije-na-internetu/> (last visited 4 April 2019)
- Perry S & Roda C (2017) *Human rights and digital technology: Digital tightrope* London: Palgrave MacMillan
- RCUB Istorijat (trans Serbian: The History) *Računarski Centar Univerziteta u Beogradu* (trans Serbian: IT Centre at the University of Belgrade), available at <https://www.rcub.bg.ac.rs/o-rcubu/istorijat.html> (last visited 28 April 2019)
- Senkić D (2015) Facebook.com, available at <https://www.facebook.com/danijel.senkic.3/posts/10206446620113660?fref=nf> (last visited 4 April 2019)
- Share Foundation (2019) 'New surveillance cameras in Belgrade: Location and human rights impact analysis – "withheld"' SHARE Foundation, available at <https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/> (last visited 4 May 2019)
- Share Foundation (2015) Vodič: Osnove digitalne bezbednosti. SHARE Foundation, Belgrade
- Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights 1984
- Soh C, Connolly D & Nam S (2018) 'Time for a fourth generation of human rights?' UN Research Institute for Social Development, available at <http://www.unrisd.org/TechAndHumanRights-Soh-et-al> (last visited 28 April 2019)
- Trusted Introducer : Directory : SRB-CERT nd, available at <https://www.trusted-introducer.org/directory/teams/srb-cert.html> (last visited 4 May 2019)
- UN Sustainable Development 'Transforming our world: The 2030 Agenda for Sustainable Development' UN Sustainable Development Goals, available at <https://sustainabledevelopment.un.org/post2015/transformingourworld> (last visited 28 April 2019)
- UN Human Rights Committee General Comment 34 Article 19: Freedom of opinion and expression, 2011 CCPR/C/GC/34

- Universal Declaration of Human Rights 1948, available at <https://www.un.org/en/universal-declaration-human-rights/> (last visited 4 April 2019)
- Valich T (2008) 'Croatian Facebookers protest: 4 000 people in Zagreb, police/political disruption in smaller cities', available at <http://vrworld.com/2008/12/06/croatian-facebookers-protest-4000-people-in-zagreb-policepolitical-disruption-in-smaller-cities/> (last visited 28 April 2019)
- Werman M (2008) 'Facebook protests in Croatia' Public Radio International, available at <https://www.pri.org/stories/2008-12-05/facebook-protests-croatia> (last visited 4 May 2019)
- Yesil B, Sözeri EK & Khazraee E (2017) 'Turkey's internet policy after the coup attempt: The emergence of a distributed network of online suppression and surveillance' Internet Policy Observatory

Big Brother in the Middle-East and North Africa: The expansion of imported surveillance technologies and their supportive legislation

Ola El-Ashy,* Ilaria Maroni, Hazem Mizyed,***
Razan Nammar**** and Mohammed Al-Maskati*******

Abstract: *The article analyses digital surveillance companies and the possibilities that technology makes available to oppressive regimes: from monitoring centres facilitating mass surveillance on all telecommunications, to firewalls that filter what users can access, and spyware that tap into the information stored in any personal device connected to the internet. This grim picture of new technologies becomes significantly darker when taking into account the volume of this 'international repression trade' and the market value of surveillance companies operating in states self-identified as democracies.*

Key words: *digital rights; surveillance; cyber-crime legislation; right to privacy; freedom of expression; national security; cyberwar; information technology; human rights defenders*

1 Introduction

Digital rights no longer are a simple extension of human rights. They have become central components of several rights: digital media for the right to information; social media for the right to free assembly; cybercommunication for the right to privacy; and so forth. Parallel to these developments, cyberspace has become a crucial arena for political action but also for repression. Activists use it to share information and to mobilise, while repressive governments have been resorting to surveillance technology in order to suppress social movements, and to identify and apprehend activists and dissidents.

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. MA holder (Arab Masters for Democracy and Human Rights), Human Rights and Legal Researcher; olaelashi93@gmail.com

** MA (Democracy and Human Rights in the MENA Region), MA (International and Diplomatic Affairs); Reporter, freelancer; ilaria.maroni@hotmail.it

*** MA (Human Rights and Democratisation); social entrepreneur interested in new technologies; Hazem.mizyed@gmail.com

**** MA (Democracy and Human Rights), MA (Democratic Governance – Rule of Law in the MENA Region); International Law Consultant, freelancer; r.namari@live.com

***** MA (international studies), Digital security expert, MENA Digital protection Coordinator for Front Line Defenders; mohdmaskati@protonmail.com

Authoritarian governments depend on cyber-surveillance companies based in democratic countries, which are developing and exporting sophisticated software needed to monitor electronic device activities and data stored on hard drives, or intercept data transmitted over wireless or cable networks. Surveillance technologies can map relationships, recognise patterns, and analyse discourse. They can target different types of data: Audio and video surveillance tap into household and corporation surveillance camera systems. Phone monitoring gathers data communicated across mobile, fixed or next generation networks. Location monitoring intercepts the location of a target using phone identifiers or tracking devices. Internet monitoring technologies gather information communicated across the internet, often on a mass scale. This can be done through monitoring centres that hack into internet communications, telephones, computer networks and databases using several tools. Intrusion is a tool that works through the installation of spyware on communication devices that can extract data and control functions. Biometrics software allows individuals to be monitored through the identification and recognition of their physiological or behavioural characteristics. Bug detection tools allow counter-surveillance (Privacy International 2016).

Even though some parts of the Middle East and North Africa are lagging behind technologically, authoritarian regimes have generally upgraded their control and repression mechanisms through the use of sophisticated digital surveillance technologies. The restriction on digital rights, most notably freedom of expression, the right to privacy and the right to information, is further supported by new legislation that aims to silence human rights defenders and activists calling for democratisation. We will first look into the exportation and use of digital surveillance technology through the study of three companies originating and functioning in countries that are considered democratic: Amesys, Netsweeper and the NSO group, headquartered in France, Canada and Israel respectively. We next examine how some states in the Middle East and North Africa that are importing these technologies are enacting anti-cybercrime laws to reap the full benefits of these technologies, focusing on Palestine, Jordan, Egypt and Bahrain.

2 Exporting surveillance technologies

The first part of this article examines three companies based in self-identified democracies that export different types of surveillance technologies to authoritarian regimes: French Amesys produces mass surveillance technologies to monitor communications on specific networks; the Canadian Netsweeper provides technologies and services for internet content filtering and blocking; and the Israeli NSO Group infects targeted devices through spyware that extracts data.

3 Monitoring centres: The case of the French Amesys

'We are in a world now where not only is it theoretically possible to record nearly all telecommunications traffic out of a country, all telephone calls, but where there is an international industry selling the devices now to do it' (Wikileaks.org nd). This statement by Julian Assange was well

illustrated in an Amesys brochure that Wikileaks had found and published in 2011. One of its illustrations shows the difference between lawful interception that only tracks internet protocol addresses and the mass surveillance that the company proposes which allows the monitoring of the whole traffic on any given network, regardless of data format (audio, video or text). The services that this French company offers do not require the hacking of individual devices through the use of malicious software but monitors the national network, or any specific network, through the use of keywords (Wikileaks.org 2011).

Following the fall of Muammar Gaddafi's regime in Libya, an abandoned monitoring centre in Tripoli was discovered containing Amesys training manuals and posters. One of the posters about the Eagle system read: 'Whereas many internet interception systems carry out basic filtering on IP address and extract only those communications from the global flow [legal interception], Eagle Interception system analyses and stores all the communications from the monitored link [massive surveillance]' (Garcia et al 2015). The Libyan authorities had been using a Deep Packet Inspection technology and analysis software developed by Amesys. In an interview published by the French newspaper *Figaro* in September 2011 a former official of the Libyan External Security Organisation explained that the system was able to find 'targets within the country's massive flow' and to identify 'individual suspects using keywords'. This witness summed it up as follows: 'We listened in on the entire country.' The system was subsequently used to create data analysis methods that were applied to the collected data to hone keywords used for queries and to monitor the findings obtained collaboratively with Libyan authorities, in particular the Libyan military high command' (FIDH 2014).

Amesys had sold to the Libyan government the telecommunication surveillance system called Eagle, as a 'favour' on behalf of the French President (Tesquet 2017). This technology was allegedly used in the tracking and torturing of dissidents and activists. It allowed the Libyan authorities to confront dissidents and activists with private social media texts and emails (FIDH 2014). This sale took place following Libyan leader Muammar Gaddafi's visit to France in 2007. At that time, the International Federation for Human Rights and the Libyan League for Human Rights were pressuring the government not to support a regime responsible for 'serious human rights violations' by either 'tolerating' or directly committing such violations. This action did not prevent the sale or discourage the two civil society organisations from pursuing their pressure. In 2011 they filed a complaint which sparked an investigation into the sale of this technology (FIDH.org 2015). Shortly thereafter the company rearranged its operations. Stephan Salies, owner of Amesys, created two new companies with different names: Advanced Middle East Systems based in the United Arab Emirates (UAE), and Nexa Technologies in France. They improved the Eagle system and called it Cerebro with reference to a tracking device used in the X-Men science fiction series (Tesquet 2017). Their technical documentation 'promises "real-time surveillance of suspects", thanks to particularly intrusive sensors capable of tracking emails, text messages and accessing chat rooms and social media sites'. It adds that 'investigators can follow their target's activities by entering advanced criteria (email address, telephone numbers, keywords)' (Tesquet 2017). In 2017 Nexa Technologies made headlines by selling surveillance technology to Egypt. Cerebro had been gifted to Egypt by the

Emirati government. According to the French daily *Le Monde*, the UAE purchased for €10 million a monitoring system which was to be directed against the Muslim Brotherhood. 'In a nod to the pyramids, the operation was code-named Toblerone' (Tesquet 2017).

4 Canadian firewall and filters: The case of Netsweeper

Netsweeper provides internet filtering services to individuals, corporations and governments. On the website of this Canadian company, their products are associated with the rise in 'cyber-threats, cyber-crime, hacktivism, the proliferation of illicit content and attacks on critical infrastructure and intellectual property' (Netsweeper.com nd). The application of online filtering technologies determines the landscape of the internet with which the user can interact. Artificial intelligence (AI) offers 'dynamic classification and categorisation, which optimises network usage while providing a positive, productive, and safe internet experience' (Netsweeper.com nd). Indeed, the use of filtering technologies is varied. They are used by schools and universities to create a 'safe environment' for students. Internet service providers can filter websites harbouring criminal content linked to terrorist groups or child pornography. However, in all cases filtering technologies offers control over the content that is accessible on the network. This raises concerns related to freedom of thought, speech and action, with an intensity commensurate to the level to which this control is exerted.

The use of pre-set filters becomes particularly problematic when states use them to block a certain type of online content from their country. Netsweeper offers multiple filtering categories from which the customer can choose. The categorisation occurs in more than 30 languages, and they are driven by AI and human review. As the Citizen Lab explained: 'A network administrator need only select a given content category – such as 'gambling' or 'hate speech' – and all content categorised as such will be blocked. Creating this database of websites and the ongoing process of categorisation is a substantial undertaking (The Citizen Lab 2018). The company claims that it has categorised over 10 billion uniform resource locators (URLs) and that it categorises 22 million new URLs each day (Netsweeper.com nd). By 2022 it is estimated that the value of the web content filtering market will be US \$3,8 billion (The Citizen Lab 2018).

Netsweeper claims centralised control over its products. However, it has multiple distributing partners around the world and has branches in the Middle East, South America and the United States. Its software is installed on public networks in Bahrain, Pakistan, Qatar, Somalia, United Arab Emirates and Yemen (The Citizen Lab 2018). In the UAE, Netsweeper's filters categorise the entire World Health Organisation website as pornographic; and so are the websites of the Christian Science Monitor, the World Union for Progress Judaism, the Centre for Health and Gender Equity, and Change Illinois (Pangburn 2018). After criticisms relevant to the technologies enabling the blocking of lesbian, gay, bisexual, transgender and questioning (LGBTQ) and HIV-related content or pages categorising them as pornographic, Lou Erdelyi, Netsweeper's chief technology officer, explained that '[a]s of December 25th, 2018, Netsweeper no longer has a category titled LGBTQ+ nor does it block such content' (Pearson 2019). The company also claims less categorisation

relevant to the category of ‘alternative lifestyles’. Nevertheless, there are concerns about the use of these technologies in countries considered authoritarian. While Netsweeper’s technologies are often used for purposes of safe internet browsing, such as blocking child pornography websites or websites considered inappropriate for school internet, they also often are used by authoritarian regimes to block websites of opposing political views, and human rights-related content.

5 Intrusion technologies from Israel: The case of the NSO Group

In December 2018 an Israeli cyber-security company, NSO Group, gained media attention when Omar Abdulaziz, a Saudi dissident, accused it of infiltrating his smartphone. Abdulaziz pressed charges, claiming that the firm had sold its signature spyware to the Saudi government and given access to his conversations with Jamal Khashoggi. According to the lawsuit, this played a major role in ‘the decision to murder’ the *Washington Post* columnist and political opponent who was lured into the Saudi consulate in Istanbul and dismembered (Kirkpatrick 2018).

It was not the first time that the NSO Group came under the spotlight. In fact, after operating in the shadows for years, Citizen Lab brought it to light. Citizen Lab is an interdisciplinary laboratory at the Munk School of Global Affairs and Public Policy at the University of Toronto. It is tasked with producing ‘evidence-based research on cyber-security issues that are associated with human rights concerns’, using a ‘mixed methods approach to research combining practices from political science, law, computer science, and area studies’ (The Citizen Lab 2018). Academics at the Citizen Lab receive financial support from a vast range of donors, including the Canada Centre for Global Security Studies and Open Society Foundation. This internet ‘watchdog’ reported in 2016 that Ahmed Mansoor, a human rights activist living in the UAE, had received a text message with a suspicious link. Mansoor forwarded it to the task force and they were able to uncover what a cyber-security firm described as ‘the most sophisticated, targeted, and persistent mobile attack ever found on iOS’, and traced it back to the NSO Group (Lookout.com 2016). We will look into how a small Israeli start-up turned into one of the most controversial partners of Arab authoritarian governments in less than a decade.

The NSO Group is high-ranking among so-called ‘internet mercenaries’ (Mazzetti et al 2019). It was established by two high school and army friends, Shalev Hulio and Omri Lavie, who sought to break into encrypted communications by developing software that could hack smartphones. The company came into existence only two years later with the expertise of the Israel Defence Force’s Unit 8200, of whom Hulio and Lavie are believed to be veterans (Brewster 2016). Unit 8200 is the equivalent of the US National Security Agency (NSA). It is an intelligence unit in the front lines of Israel’s cyber-wars. According to Israeli investigative journalist Yossi Melman, one can find Unit 8200 ‘whenever there is a very significant or risky operation ... Even days or weeks before the actual operation taking place. There is not a single major Israeli intelligence operation in which Unit 8200 is not involved’ (Behar 2016). Allegedly, this unit was responsible for infecting computers at Iran’s Natanz uranium enrichment

facility with Stuxnet, a worm created in cooperation with the NSA and the Central Intelligence Agency (CIA) (Behar 2016).

This unit of the Israeli army is not only involved in international warfare but also in the daily occupation of Palestinian territories. As such, it is also engaged in managing the daily lives of Palestinians living in the West Bank and under blockade in the Gaza Strip. In 2014, 43 former soldiers and active reservists spoke out, revealing how they were responsible for collecting an extensive range of electronic communications from Palestinians, such as 'email, phone calls and social media in addition to targeting military and diplomatic traffic' (Beaumont 2014). Long before experts raised doubts about the potential risks of technology use for human rights, Unit 8200 started enacting massive surveillance and espionage at the expense of 'innocent people unconnected to any military activity'. Other testimonies published stated: 'On a personal level, there is no respect for Palestinian privacy'; 'if anyone interests us, we'd collect information on his or her economic situation and mental state ... in order to turn them into a collaborator or something of the sort'; and 'whether said individual is of a certain sexual orientation, cheating on his wife, or in need of treatment in Israel or the West Bank – he is a target for blackmail' (*The Guardian* 2014). The 43 *refuseniks* were quickly expelled from the Unit for crossing 'a red line' and acting 'inappropriately' (*The Guardian* 2015).

In early 2011 the company tested the first version of *Pegasus*, its signature spyware software. Its website claims that its technology 'helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe' against 'terrorists, drug traffickers, paedophiles, and other criminals' and 'the world's most dangerous offenders'. *Pegasus* is spyware that acts in the background to extract private information. It usually installs itself through malicious texts and emails, or public wi-fi networks (Perlroth 2016). In late 2016 the *New York Times* received internal NSO Group correspondence and contracts from two sources close to the company. The article lists the price of surveillance: starting from a \$500 000 installation fee, an extra \$650 000 for access to ten iPhone users; \$650 000 for ten Android; \$500 000 for five BlackBerry; and \$300 000 for five Symbian (Perlroth 2016). Six months later the Israeli newspaper *Haaretz* wrote that the Saudis agreed to pay 55 million for the *Pegasus 3* (Harel et al 2018). For this price, *Pegasus* can extract text messages, contacts, e-mails, GPS locations and passwords; it can record and listen to phone calls, and even turn on the microphone and the camera on a smartphone. What is distinctive about this product is the complete absence of footprint: It is almost impossible to discover, and it has a 'self-destructive' feature that destroys all traces if detected (Franceschi-Bicchierai et al 2018).

In order to prevent the technology from 'falling into the wrong hands', NSO Group co-president Tami Shachar explained in an interview that the company has three levels of vetting (Stahl 2019). As cyber-surveillance technology sales are equivalent to arms exports, the Israeli Defence Ministry needs to approve every potential customer. However, so far there is no evidence of any rejection. The company has also created a business ethics committee, which had denied sales to Turkey but not to Mexico and Saudi Arabia (Mazzetti et al 2019). Lastly, every client must sign a

‘contractual agreement’ in which they declare that ‘the only intended use of the system will be against terror and crime’ (Stahl 2019).

Under this legal vacuum and lack of accountability, Pegasus has infected devices in possibly as many as 45 countries (Marczak et al 2018). Between August 2016 and August 2018, researchers found more than a thousand IP addresses and domain names related to the Israeli firm’s ‘dirty work’ (Marczak et al 2018). Two important cases have revealed its *modus operandi*: one in the UAE and one in Mexico. The first case is that of Ahmed Mansoor, a world-renowned activist who is currently serving a 10-year prison sentence for expressing his criticism of the Emirati government’s human rights abuses. After more than a year in prison without trial, he was condemned on charges of disseminating fake news online and jeopardising the country’s reputation (Front Line Defenders 2019). His health is deteriorating and appeals from Human Rights Watch, Amnesty International, Frontline Defenders and others have so far remained unheard. In the summer of 2016, while on a *de facto* travel ban with his passport having been confiscated by the authorities (Human Rights Watch 2019), Mansoor received a suspicious text containing a link that promised ‘new secrets’ about detainee conditions in UAE. Mansoor did not fall for the bait. Instead, he sent the message content to the Citizen Lab that was able to trace it back to the NSO Group and their attempt to install Pegasus on the activist’s iPhone.

In June 2017 the *New York Times* broke the news on how the Mexican government was using NSO Group’s technology against citizens who were neither terrorists nor criminals. The media outlet revealed that Pegasus had infiltrated the devices of lawyers, anti-corruption activists, journalists and civil society representatives (Ahmed et al 2017). In the same hours, the Citizen Lab posted its comprehensive findings: Victims, including media and television personalities, non-governmental organisation (NGO) members, and even the under-age son of a reporter, received fake messages containing the spyware (Scott-Railton et al 2017). Following the public outcry, then President Enrique Peña Nieto responded with a letter to the *New York Times*, denying all accusations and stating that there was no evidence that the Mexican government was behind the surveillance (Beauregard 2017).

Throughout 2018 Pegasus’s attacks increased, and so did attention from public opinion and media, which started questioning cyber-security companies and governments buying their technology. The NSO Group’s products were used to infiltrate devices of Amnesty International staff (Ingleton 2018), which quickly prompted the Israeli Ministry of Defence to withdraw licences for the firm (Amnesty International 2018). Saudi Arabia was the most prolific customer, with many attempts on dissidents living abroad, such as Ghanem Almasarir, a comic in London (Stahl 2019), and Omar Abdulaziz.

Since Jamal Khashoggi’s murder in the Saudi consulate in Istanbul, the NSO Group has focused all its efforts on rebranding (Franceschi-Bicchierai 2019). Under a new marketing strategy to make the company appear more appealing and transparent, co-founder and CEO Hulia declared on television that Pegasus prevents ‘crime and terror’ saving ‘tens of thousands of people’ and helping ‘create a safer world’ (Stahl 2019). When asked about the role of his company in the killing of the Saudi dissident, he evaded the question, saying that he was not willing to ‘talk about

specific customers'. Other public relation moves consist of allowing cameras inside their once-secretive headquarters in Herzliya, creating a brand-new website, and releasing public statements after any allegation made by the media. Current estimates value the NSO Group around \$1 billion (Haaretz 2018). Not all the rebranding efforts are succeeding. At the beginning of 2019, AP News broke the story of individuals using fake names and affiliations who contacted two Citizen Lab researchers investigating the NSO Group. The academics were filmed while they were being questioned about Israel, anti-Semitism and religion. Although no connection with the NSO Group was proven, these tactics recall the assignments of the Black Cube, a private Israeli intelligence agency, tasked with harassing Harvey Weinstein's accusers (Satter 2019).

Although producing different surveillance technologies, the NSO Group, Amesys and Netsweeper operate with a similar pattern. The three companies are all based in democratic countries, but that does not prevent them from selling their products to authoritarian governments with little control or accountability. In fact, most of their activity is kept hidden from public scrutiny. Nevertheless, the multiple scandals surrounding the sale of surveillance technology to authoritarian governments, especially the judicial case that was opened against Amesys, drew more attention aimed at better regulating the export of surveillance and dual-use technologies. The Wassenaar Arrangement is the main regulatory regime for such technologies. '[It] has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies' (Garcia et al 2015). It stipulates which military and dual-use goods (that have both military and civilian use) should be subject to licensing and has 41 participating states, including Russia, Japan, the US and the member states of the European Union. However, the list of items is also used by a large number of non-signatory states as part of their own licensing regulations, including Israel and China (Privacy International 2016).

As technology progresses, the regulation of exports of digital surveillance needs to be continuously updated. The EU Dual-Use Regulation 429/2008 restricts the export of specialised large-scale IP monitoring systems. The French government specifically pushed for export control mechanisms within the European Union that would regulate Amesys's technology and it implemented these regulations immediately after their adoption by Wassenaar in 2013 (FIDH.org 2015). Nevertheless, Amesys was granted nine other licences since the beginning of 2016: three in West Africa, two in the Middle East, one in sub-Saharan Africa, one in Europe, one in Asia and one in South America. The surveillance technologies arms race goes on. As a person in the business confided (Tesquet 2017):

Of course the French services subcontract technical intelligence. It's either that or handing control to the Chinese or the Israelis. We aren't Care Bears. We tell ourselves we are doing it in the interests of our country. In any case, all the countries are equipping themselves, whether it's through us or elsewhere.

The exportation of digital surveillance tools sometimes is referred to as the international repression trade (Privacy International 2016). Born over four decades ago, it has expanded exponentially in the last decade, yet reliable

data remains scant. Nevertheless, the trade volume of surveillance technologies is estimated (CAUSE, 2015) between US \$5 and \$12 billion (Kirkpatrick 2019). This probably explains the failings of international regulations and the national legislation of countries that export surveillance technologies. However, they are also supported by the political needs of the importing governments that have been developing and upgrading their legislation in an effort to regulate the internet and cyber-space usage, but also to fully benefit from the features and results that those powerful weapons provide.

6 Domestic legal support systems for surveillance: Middle Eastern cyber-crime legislation

Governments in the Middle East and North Africa have been updating their legislation relevant to cyber-crimes following a similar repressive pattern meant to support the use of surveillance technologies. This has led to a trending practice of persecuting journalists and activists for views and posts shared on social media platforms. With the widespread use of social media in recent years, some states have dealt suspiciously with journalists, bloggers, human rights defenders and activists, and started to censor criticism towards public figures. Some authorities have detained, interrogated, prosecuted and, in some cases, physically harmed internet users due to their posts. Imported surveillance technologies play a central role in this repression as they allow the identification of critics and political opponents, and the gathering of data that can be used against them. However, in order to prosecute them a new legislation needs to be drafted, allowing the state to qualify their actions as offences. We will look into how this legislative process is unfolding in Bahrain, Egypt, Jordan and Palestine, and the specific tools used to support repression, namely, vague terminology, numerous regulatory bodies and the possibility of shutdowns.

7 Vague cyber-offences and creeping cyber-crime laws

There is a striking similarity between two cyber-crime laws enacted recently in the Middle East; those of Jordan and Palestine. The similarities go beyond their content and into the way in which they were actually adopted. Both states passed them without a public consultation or debate. However, this approach meant to bypass civil society and stifle any opposition to them. Both legislation was met with opposition from civil society organisations (CSOs) that considered them a breach to the right of freedom of expression and opinion.

In 2015, the Jordanian government introduced draft cyber-crime legislation, intended to update the Information Systems Crime Law of 2010 (House 2016). It was met with immediate condemnation from CSOs. Protests flared for two years when this legislation was used to sentence six journalists to six months imprisonment and a fine of \$80 000 (Ersan 2018). The journalists had been arrested due to a complaint by Secretary-General Youssef Issawi to the Anti-Cyber Crime Unit at the Public Security Directorate for a video shared on Facebook accusing him of 'appropriating government funds and state lands to build a road to his palace'. Protestors argued that the law infringed on the right to privacy, freedom of

expression and digital rights. In December 2018 these protests resulted in the government withdrawing the 2015 law for further amendments (Now 2019). Two days later, the Jordanian government presented to the Parliament an amended law, once again without engaging with CSOs. The amendments expanded the scope of cyber-crime to encompass hate speech. It also increased the penalty from one week to three months' and up to one year's imprisonment and raised the fines for perpetrators from \$140-\$280 to \$700-\$1 400. The amendments raised concerns among human rights activists and advocates who feared that the Bill would restrict freedom of speech online. In November 2018, Jordanian activists launched a social media campaign, calling on the government to withdraw the cyber-crime law.

In February 2019, the Jordanian Parliament voted in favour of amending certain clauses of the law, in particular the clauses on hate speech and fake news. The definition of hate speech that it introduced was vague, stating that 'every writing and every speech or action intended to provoke sectarian or racial sedition, advocate violence or foster conflict between followers between different religions'.

Activists, journalists and human rights defenders perceived this vagueness of terms as an increased threat and feared that the government would use this law to prosecute its critics. It blurred the lines between hate speech, criticism of public figures and freedom of opinion and expression (Times 2019).

In Palestine the cyber-crime legislation was enacted in June 2017 through a Presidential Decree. In several of its 61 clauses, Cyber-Crime Law 16 allows disproportionate and indiscriminate infringements on several rights, including freedom of expression and opinion, the right to privacy and access to information. The Law uses vague terms to describe several offences, such as 'threat to national security', which can lead to harsh imprisonment sentences and excessive fines for online criticism. Some clauses of the Law, particularly articles 32, 33 and 34, authorise surveillance of social media users and blocking websites and pages without a court warrant. Security services can easily force internet providers to disclose their customers' data, even if this breaches the company's code of conduct and violates the customer's privacy (Advancement 2018). It has also become common practice for Palestinian security services to force civilians to disclose their passwords to access their personal pages and deliberately interfere with what they post (Watch 2018).

The enactment of the Law came about without previous consultation with CSOs or a public debate. Based on this Law, especially its article 20, journalists, activists and human rights defenders were arrested for propagating news that allegedly threatened national security (Ayad 2018). The adoption of the cyber-crime law increased the scope of repression allowing security forces to prosecute and silence voices due to loose clauses and vague terminology (Watch 2017). Immediately upon the enactment of the Law, a large-scale surveillance campaign was carried out against independent and opposition news websites in the West Bank. In one month alone, internet providers blocked 29 websites following an official order issued by the Attorney-General of Palestine, Ahmad Barrak (Odeh 2018). On 4 June 2017 Palestinian security forces detained a Palestinian journalist, Taher Al-Shamali, for publishing an article that criticised the Palestinian President. He was charged with 'insulting higher

authorities and causing strife'. Nasser Jaradat, a media student, was also arrested for sharing Al-Shamali's article on his Facebook page. Both were detained for 15 days under the same charges (AbuShanab 2017; Abdelbaqi 2016).

Human rights organisations campaigned against the cyber-crime law and demanded its immediate suspension. This demand was raised in a session at the office of the Palestinian Liberation Organisation (PLO) in Ramallah, where a coalition of 11 organisations submitted their comments and objections to Hanan Ashrawi, the head of the PLO Department of Culture and Information (Musawa 2017). This action led to the Ministry of Justice organising governmental consultations with CSOs to discuss possible amendments to the Law. Some amendments were adopted, but these were minimal, and the Law remained vague and prone to infringe on freedom of expression and opinion and digital rights, under the pretext of combating cybercrimes (Ayad 2018).

The Palestinian anti-cybercrime legislation is not the only framework through which the freedom of expression and opinion in cyber-space is breached in Palestine. The country is not a sovereign state and is divided into two entities governed by rival Palestinian factions. The Gaza Strip is governed by Hamas and is under Israeli blockade, while the West Bank is governed by Fatah and is under Israeli occupation. This means that the Palestinian authority's legal instruments and practices are not the only ones to directly impact Palestinian lives, their digital rights, freedom of expression and access to information. In recent years, Israel has been manipulating and pressuring social media giants such as Facebook and YouTube, to remove posts and block personal and official Palestinian pages under the guise that they 'incite' against Israel (Odeh 2016). This goes contrary to the International Covenant on Civil and Political Rights (ICCPR), particularly article 19 (UN General Assembly 1966) in its General Comment 34 which states that offences 'such as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying" or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression'. The compliance of Facebook and YouTube with the Israeli government's requests undoubtedly restricts freedom of expression, reducing the role and the capacity of social media and internet platforms, and preventing journalists from accomplishing their work on informing the general public (Odeh 2016).

At the same time, criticism on social media of Fatah and Hamas among media activists, human rights defenders and the public in general is met with firm actions by Palestinian security forces (Watch 2018). These actions sometimes lead to the detention and torture of journalists and activists giving rise to self-censorship on social media and internet platforms (Odeh 2016). The Palestinian government had targeted journalists and activists who opposed or criticised the government prior to the enactment of the cyber-crime law, prosecuting them under the Penal Code. Similarly, in Gaza freedom of expression has declined sharply since the internal political divide, in 2007. Hamas uses different forms of restrictions against journalists and activists, including detention, threats and torture, to stifle any element that criticises or threatens its rule.

8 The multiplication of regulatory bodies and the instrumentalisation of internet technology companies

Some anti-cybercrime legislation in the region have relied on legal techniques other than 'vague terminology' to ensure stronger control over cyber-communication and social media. Bahrain, for example, set up several regulatory bodies to monitor and prosecute dissenters. Egypt has transformed internet service providers into control agents executing the government's policies. The establishment of regulatory bodies and the transformation of information technology (IT) companies into regulatory agents are not the only tools governments use to 'regulate' internet use. They sometimes resort to non-regulated shutdowns of local or national communication systems in an effort to silence the opposition.

In Bahrain the government has over the years gradually introduced several restrictive instruments varying from laws and regulations, governmental bodies, and surveillance software to monitor citizen activities online. These instruments are allegedly meant to safeguard national security and order. However, they resulted in a massive crackdown on internet users that reveal their intention to silence political dissidents (Bahrain Centre for Human Rights 2018).

Bahraini authorities practise surveillance and censorship through several laws and regulations. The government passed the Press Law 47/2002, which regulates both online and print media. This law allows strict control on the circulation of sensitive topics. Article 19 prohibits the publication of any content 'instigating hatred of the political regime, encroaching on the state's official religion, breaching ethics, encroaching on religions and jeopardising public peace' (Bahraini Journalists Association 2019). The Minister of Information issued Decree 68/2016, which further restricts the distribution of electronic media and empowers the state to target and prosecute content publishers (Bahraini Journalist Association 2019). In 2014 Bahrain passed its national cyber-crime legislation under Law 60/2014 on Information Technology Crimes. The Law is complementary to the Media Regulation Law of 2002, as it provides in article 23 penalties for infringing the complementary regulations (Bahraini Journalists Association 2019).

The government did not limit itself to drafting new laws and regulations. It also created governmental bodies to monitor cyber-activities: the Information Affairs Authority, established in 2010; the General Directorate of Anti-Corruption and Economic and Electronic Security, established in January 2011; and the Cyber Safety Directorate, established in November 2013. The Information Affairs Authority (IAA) is responsible for monitoring all media outlets in Bahrain, whether printed or online media, to ensure their compatibility with media regulations. It has the authority to block any website or content for allegedly 'instigating hatred of the political regime, encroaching on the state's official religion, breaching ethics, encroaching on religions and jeopardising public peace or raising issues whose publication is prohibited by the provisions of this law' (Bahraini Journalist Association 2019). The Ministry of Interior set up another monitoring authority, namely, the General Directorate of Anti-Corruption and Economic and Electronic Security. This authority tracks internet users who violate the media regulation laws, and opens an investigation of those who offend, defame and insult others online. The

Directorate has summoned and interrogated human rights defenders, political activists and social media activists over charges of insulting or offending a governmental body, the King, or a neighbouring country (General Directorate of Anti-Corruption and Economic and Electronic Security 2019). The third governmental body was set up by the Ministry of Telecommunications Affairs. The mandate of the Cyber Safety Directorate is to 'assume its role in monitoring websites and social media networks to ensure they are not used to instigate violence or terrorism and disseminate lies and fallacies that pose a threat to the kingdom's security and stability' (Bahrain Centre for Human Rights 2013). In addition, a hotline and an email address were published for the general population to report any infringement of the 'right cyber-agenda' as regulated by the laws (Bahraini Ministry of Interior 2013).

The legislation and governmental bodies that were set up to 'regulate' cyber activity actually curb freedom of expression and the right to information. Criticism of the royal family and sometimes of the political and economic situation is not tolerated. Activists were arrested for sharing satirical content opposing the regime. For example, a women's rights activist, Ghada Jamsheer, was arrested in 2014, her blog and Twitter account were blocked, and she was sentenced to a year in prison for defamation and insulting the royal family through a tweet she posted about corruption in a hospital managed by a royal family member (Bahrain Centre for Human Rights 2015). Similarly, the president of Bahrain's Centre for Human Rights (BCHR), Nabeel Rajab, was arrested in 2016, allegedly for disseminating false news on his Twitter account when he published a report on torture incidents in Bahrain's prison and violations committed by the Saudi Coalition forces in Yemen (Bahrain Centre for Human Rights 2016). This type of censorship is supplemented by another one that targets websites: Over 1 000 websites were blocked 'for sharing illegal content', and so was an encrypted messaging and Voice over IP service such as Telegram in 2011 (The Verge 2019) and prominent live streaming services broadcasting Shiite religious ceremonies such as PalTalk and Matam.tv in 2013 (Reporter-ohne-grenzen.de 2019). Not surprisingly, a United Nations (UN) spokesperson at the Human Rights Council in Geneva noted that Bahrain had failed to obey 176 of the Council's recommendations (Civicus.org 2017).

In Egypt the government not only blocked websites, but shut down all communication systems in an effort to curb the mobilisation efforts of the opposition forces and isolate the protests from the world's attention at the wake of the Arab Spring. Indeed, the government obliged telecommunication companies in January 2011 to shut down the internet, and voice and texting services. In 2014 the Egyptian government used a surveillance system called 'See Egypt' to monitor the internet activity of activists, tapping into their email accounts and Skype calls (Buzzfeed News 2018). This surveillance system penetrates laptops remotely and access personal data, such as pictures, passwords and files. It can also operate cameras and microphones to record conversations. It was used against Esraa Abd El- Fatah, a prominent human rights activist, who had her personal photos, email and phone calls leaked on Facebook. This was used to 'expose her indecency' and undermined her credibility (Freedom House 2018).

In 2018 the President of the republic ratified Law 180, an anti-cyber-crime law directed towards users and internet service providers, further restricting digital rights. Article 7, for instance, allows the blocking of websites accused of publishing content constituting a threat or a crime against national security and the economy. Also, it obliges internet service providers to block access to the website within 48 hours whenever notified. This allowed the blocking of 500 websites in March 2018 under the claim of disseminating fake news (Access Now 2018). This anti-cyber-crime legislation also focuses on regulating social media discussions. It provides that any user with 5 000 followers can be considered as operating a media platform and could be held accountable for sharing 'fake news'. Consequently, it led to the imprisonment of Facebook users for the dissemination of unfavourable opinion (BBC News 2018). Such was the case of Masoum Marzouk, a former diplomat, who had called for early presidential elections on his Facebook page (BBC News 2018). Article 9 of the Law authorises internet service providers to store their customers' information and data, such as messages, website visits and telephone calls, up to 180 days and to hand it to the authorities when requested (IFEX 2018). This provision was translated into reality when the government requested Uber and Careem car services to hand over their customers' data (Mada Masr 2018). Allegedly, the purpose of this legislation and policy is to counter terrorism. Nevertheless, they contradict article 57 of the Egyptian Constitution which states:

The right to privacy may not be violated, shall be protected and may not be infringed upon. The state shall protect citizens' right to use all forms of public means of communications. Interrupting or disconnecting them, or depriving the citizens from using them, arbitrarily, is impermissible. This shall be regulated by law.

Internet shutdowns not only affect the social interaction and communication between individuals, but also have major negative implications on the economy. Internet disruptions caused great losses to the global economy estimated at US \$2,4 billion between July 2015 and July 2016 (Brookings Institution 2016). In Egypt the five-day internet shutdown meant to disperse protesters generated a loss estimated at \$90 million. In Bahrain the government shut down mobile internet services in the Duraz area following protests against the government's decision to revoke a Shiite religious leader's citizenship. This decision cost an estimated US \$1,2 million to the Bahraini economy (Brookings Institution 2016).

The shutdown decision not only affects political and civil rights, but also strongly impacts social and economic rights, affecting manufacturers and service providers that rely on e-commerce, cutting them off from domestic customers and global trade (Seib 2007). Even the health sector was affected by the shutdown as it disrupted communications with its suppliers (OECD 2011).

9 Conclusion

In 2011 new technologies undoubtedly supported the wave of contestation that swept over North Africa and the Middle East. When this wave toppled three regimes and shook the foundations of many others, what was then referred to as the Arab Spring was also dubbed the 'Twitter revolutions',

highlighting the important role digital social media and, more broadly, information and communication technologies played in political mobilisation and the contestation of authoritarian rule. This reflected a certain transformation of cyber-space into a public sphere, close to Jurgen Habermas's definition of a space (albeit virtual) in which citizens gather to articulate the needs of their society. Such analysis and interpretations today are much debated, but at the time they reflected a general optimistic narrative surrounding the use of information and communication technologies and the possibilities they offered.

In this article we looked into the promises of digital surveillance companies and the possibilities that technology makes available to oppressive regimes, from monitoring centres facilitating mass surveillance on all telecommunications, to firewalls that filter what users can access, and spyware that taps into the information stored in any personal device connected to the internet. This paints a grimmer picture of new technologies, one which becomes significantly darker when one takes into account the volume of this 'international repression trade' and the market value of those surveillance companies operating in states that are self-identified as democracies.

Even when there is general agreement that these surveillance technologies are powerful weapons that can be used in both civil and military terrains, their economic value for the nations that produce them, and their political importance to the nations that import them, have deeply affected the way in which governments regulate their sale and use.

On an international level, the sale of these technologies is not regulated by a treaty, but through a voluntary agreement that does not contain provisions for enforcement and compliance. Each member state to the Wassenaar Agreement develops and enforces its own control policies and only consults with other member states. The core objectives of the Agreement, namely, the promotion of transparency and greater responsibility in transfers of dual-use goods and technologies, seem to be contradicted by the sales of surveillance systems to several countries in the Middle East and North Africa. Not only are these sales not transparent, with the public never hearing about them unless information is leaked or some evidence of their criminal use is found many years after their sale; but the governments of exporting countries seem to regularly turn a blind eye to their sale to repressive governments because of the economic importance of these transactions and the wealth generated by these companies.

At the national level the use of these technologies in the Middle East and North Africa is not directly regulated by any particular law. This means that there is no particular legislation that bans or authorises the use of mass surveillance, interception technologies or filters. However, anti-cybercrime laws indirectly authorise the use of some of these technologies (that is, monitoring, filtering and banning), and inform on the repressive intentions of the legislator and the controlling character of the regulations. We have seen four indicators that can be used to determine the repressive nature of an anti-cybercrime legislation: the use of vague terminology in the definition of cyber-offences; the absence of discussions with CSOs when passing the legislation; the multiplication of regulatory bodies; and the transformation of internet service providers into control agents. These

indicators may be used as red flags when it comes to the sale of surveillance technologies.

We have also seen that public opinion and CSO mobilisation against repressive anti-cybercrime legislation or the sale of surveillance technology to repressive regimes has not been very effective. In the case of mobilisation against legislation, they can delay the enactment of anti-cybercrime laws, but have sometimes resulted in the passing of even more problematic legislation. As far as the mobilisation against the sale of repressive technologies is concerned, the media and CSOs have played a vital role in informing the public about these sales and the use of these technologies that massively violate human rights. In this regard, there are several success stories that show the importance but also the limits of such actions. The French courts put Amesys under judicial investigation in 2012 on account of the sale of surveillance technology used against political opponents to apprehend them. In 2017 the Italian Ministry of Economic Development revoked the authorisation given to several companies to sell internet network surveillance systems to Egypt following media attention and pressure from CSOs. However, these actions have not prevented authoritarian regimes from upgrading their repressive techniques through other surveillance products proposed by other companies, most of which are equally based in self-identified democratic countries. This reveals the fragility of digital rights that remain largely unprotected in both international and domestic laws, but also how this fragility directly impacts broader human rights.

References

- Tamleh (2018) *Has the Palestinian Cybercrime Law really been amended?* available at <https://www.apc.org/en/news/has-palestinian-cybercrime-law-really-been-amended> (last visited 22 April 2019)
- Abdelbaqi M 'Enacting cybercrime legislation in an endeavour to counter cybercrime in Palestine' (2016) 5 *Global Journal of Comparative Law* 226
- Access Now 'Access now' (2019), available at <https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/> (last visited 15 April 2019)
- Ahmed A 'A journalist was killed in Mexico. Then his colleagues were hacked' (2018) *Nytimes.com*, available at <https://www.nytimes.com/2018/11/27/world/americas/mexico-spyware-journalist.html?login=email&auth=login-email> (last visited 15 April 2019)
- Amnesty 'Rogue NSO Group must have licence revoked' (2018), available at <https://www.amnesty.org/en/latest/news/2018/11/israelroguenso-group-must-have-licence-revoked-over-controversial-surveillance-software/> (last visited 15 April 2019)
- Ayad C 'Policing the digital sphere: The impact of Palestine's cybercrime legislation', available at <https://archives.arab-reform.net/en/node/1384> (last visited 15 April 2019)

- BBC (nd) 'Egypt to regulate popular social media users', available at <https://www.bbc.com/news/world-middle-east-44858547> (last visited 17 July 2017)
- Bahraini Journalists 'Bahraini Journalists Association – Press law' (2019), available at http://www.bahrainijournalists.org/References_and_documents/Law (last visited 15 April 2019)
- Bahrain Rights 'Bahrain: The "cyber safety directorate" monitors internet activity in style similar to Big Brother' | Bahrain Centre for Human Rights (2013), available at <http://www.bahrainrights.org/en/node/6624> (last visited 23 June 2019)
- Bahrain Rights 'Women human rights activists Zainab Al-Khawaja and Ghada Jamsheer sentenced to prison again' | Bahrain Centre for Human Rights (2015), available at <http://www.bahrainrights.org/en/node/7540> (last visited 22 June 2019)
- Bahrain Rights 'Updates: Arrest and detention of BCHR's President Nabeel Rajab' | Bahrain Centre for Human Rights (2016), available at http://bahrainrights.org/en/updates-arrest-and-detention-bchrs-president-nabeel-rajab?_ga=2.268717169.104442301.1555430839-556041828.1554588691 (last visited 22 June 2019)
- Bahrain Rights 'Bahrain: The "cyber safety directorate" monitors internet activity in style similar to Big Brother' | Bahrain Centre for Human Rights (2019), available at <http://www.bahrainrights.org/en/node/6624> (last visited 22 June 2019)
- Beaumont P 'Israeli intelligence veterans refuse to serve in Palestinian territories' *The Guardian* (2014), available at <https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories> (last visited 22 June 2019)
- Beauregard L 'El Gobierno mexicano declaró secretos los contratos sobre el "software" del espionaje a periodistas' *El País* (2017), available at https://elpais.com/internacional/2017/06/20/mexico/1497984473_017962.html (last visited 22 June 2019)
- Behar R 'Shadow wars: In missions stretching from Iran to Syria, Israel's Unit 8200 can be (not) seen' (2016), *Forbes.com*, available at <https://www.forbes.com/sites/richardbehar/2016/05/11/shadow-wars-in-missions-stretching-from-iran-to-syria-israels-unit-8200-can-be-not-seen/#2b01c2c759ae> (last visited 22 June 2019)
- Ben-Hassine W 'Egyptian Parliament approves cybercrime law legalizing blocking of websites and full surveillance of Egyptians' *Access Now* (2018), available at <https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/> (last visited 22 June 2019)
- Bing C & Schectman J 'Special report: Inside the UAE's secret hacking team of US mercenaries' *reuters.com* (2019), available at <https://www.reuters.com/article/us-usa-spying-raven-specialreport/special-report-inside-the-uaes-secret-hacking-team-of-u-s-mercenaries-idUSKCN1PO19O> (last visited 22 June 2019)
- Brewster R 'Everything we know about NSO group: The professional spies who hacked iPhones with a single text' *Forbes.com* (2016), available at <https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#262c2f213997> (last visited 22 June 2019)
- Brookings Institution 'Global economy loses billions from internet shutdowns' 6 October 2016, available at <https://www.brookings.edu/blog/techtank/2016/10/06/global-economy-loses-billions-from-internet-shutdowns> (last visited 22 June 2019)
- Buzzfeed New 'Egypt begins surveillance of Facebook, Twitter, and Skype on unprecedented scale' (2019), available at <https://www.buzzfeednews.com/>

- article/sheerafrenkel/egypt-begins-surveillance-of-facebook-twitter-and-skype-on-u (last visited 22 June 2019)
- European Parliamentary Research Service 'STOA – Science and Technology Options Assessment', available at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf (last visited 22 June 2019)
- FIDH (The International Federation for Human Rights) 'A critical opportunity: Bringing surveillance technologies within the EU Dual-Use Regulation' (2015), available at https://www.fidh.org/IMG/pdf/cause_report_final.pdf (last visited 23 June 2019)
- Franceschi-Bicchierai L & Cox J 'Inside a demo of NSO group's powerful iPhone malware' *Vice* (2018), available at https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo (last visited 22 June 2019)
- Franceschi-Bicchierai L 'Israeli hacking company NSO group is trying to clean up its image' *Vice* (2019), available at https://www.vice.com/en_us/article/qvy97x/israeli-nso-group-marketing-pr-push (last visited 22 June 2019)
- Freedom House 'Freedom of the net' (2016), available at <https://freedomhouse.org/report/freedom-net/2016/jordan> (last visited 16 May 2019)
- Freedom House 'Freedom on the net 2018 – Egypt' 1 November 2018, available at <https://www.refworld.org/docid/5be16b1c4.html> (last visited 22 June 2019)
- Front Line Defenders 'UAE – Human rights defender Ahmed Mansoor detained' (2019), available at <https://www.frontlinedefenders.org/en/case/ahmed-mansoor-detained>. (last visited 22 June 2019)
- Gallagher R 'French company that sold spy tech to Libya faces judicial inquiry amid new allegations' (2012), available at <https://slate.com/technology/2012/06/amesys-facing-inquiry-in-france-over-selling-eagle-surveillance-technology-to-qaddafi.html> (last visited 25 June 2019)
- General Directorate of Anti-Corruption & Economic & Electronic Security .acees.gov.bh. (2019), available at <http://www.acees.gov.bh/about-acees/> (last visited 22 June 2019)
- Harel A, Levinson C & Kubovich Y 'Israeli NSO negotiated with Saudis advanced cyberattack capabilities sale, Haaretz reveals' *haaretz.com* (2018), available at <https://www.haaretz.com/israel-news/.premium-israeli-company-negotiated-to-sell-advanced-cybertech-to-the-saudis-1.6680618> (last visited 22 June 2019)
- Human Rights Watch 'Palestine: Reform restrictive cybercrime law' (2017), available at <https://www.hrw.org/news/2017/12/20/palestine-reform-restrictive-cybercrime-law> (last visited 15 April 2019)
- Human Rights Watch 'Two authorities, one way, zero dissent: Arbitrary arrest and torture under the Palestinian authority and Hamas' (2018), available at <https://www.hrw.org/report/2018/10/23/two-authorities-one-way-zero-dissent/arbitrary-arrest-and-torture-under> (last visited 18 April 2019)
- Human Rights Watch 'UAE: Free rights defender Ahmed Mansoor' (2019), available at <https://www.hrw.org/news/2019/04/12/uae-free-rights-defender-ahmed-mansoor> (last visited 22 June 2019)
- IFEX 'Egypt's cybercrime law and Media Regulation Bill violate right to freedom of expression' – IFEX (2018), available at <https://www.ifex.org/egypt/2018/09/06/egypt-cybercrime-media-regulation> (last visited 22 June 2019)
- Ingleton D 'Meet NSO Group: A go-to company for human rights abusers' *Amnesty.org* (2018), available at <https://www.amnesty.org/en/latest/news/2018/08/is-nso-group-a-goto-company-for-human-rights-abusers/> (last visited 22 June 2019)

- Jordanian Times* 'MPs reject new amendments to cybercrime law' (2019), available at <http://www.jordantimes.com/news/local/mps-reject-new-amendments-cybercrime-law> (last visited 25 April 2019)
- Julliard J 'Enemies of the internet countries under surveillance' Reporter-ohne-grenzen.de. (2019), available at https://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/2010/Feinde_des_Internets.pdf (last visited 22 June 2019)
- Kirkpatrick D 'Israeli software helped Saudis spy on Khashoggi, lawsuit says' Nytimes.com. (2018), available at <https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html> (last visited 22 June 2019)
- Lookout 'Trident zero-day iOS vulnerabilities lead to real-world espionage' (2016), available at <https://www.lookout.com/trident-pegasus-enterprise-discovery> (last visited 22 June 2019)
- Mada Masr 'Interference with uber app tied to company's refusal to share user data with security bodies' Mada Masr (blog) (2019), available at <https://madamasr.com/en/2019/01/30/feature/politics/sources-say-uber-blocked-in-egypt-for-refusing-to-share-customer-data-with-government/> (last visited 22 June 2019)
- Marczak B & Scott-Railton J 'The million dollar dissident: NSO Group's iPhone zero-days used against a UAE human rights defender' The Citizen Lab (2016), available at <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/> (last visited 22 June 2019)
- Marczak B et al 'Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries' The Citizen Lab (2018), available at <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> (last visited 22 June 2019)
- Mazzetti M et al 'A new age of warfare: How internet mercenaries do battle for authoritarian governments' Nytimes.com. (2019), available at <https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html> (last visited 22 June 2019)
- Musawa 'A legal memo to Dr Hanan Ashrawi regarding Decree-Law No (16) for 2017 on Cybercrimes' (2017), available at <http://www.musawa.ps/post/a-legal-memo-to-dr-hanan-ashrawi-regarding-decree-law-no.-16-for-2017-on-cyber-crimes.html> (last visited 15 April 2019)
- Netsweeper (nd) 'Web Content Filtering • Netsweeper', available at <https://www.netsweeper.com> (last visited 23 June 2019)
- NSO Group 'NSO Group – Cyber intelligence for global security', available at <https://www.nso-group.com> (last visited 23 June 2019)
- Odeh GB MADA (2016), available at http://www.madacenter.org/images/text_editor/FBviolationsE.pdf (last visited 16 April 2019)
- Odeh GB 'Media freedom violations in Palestine 2017' (2018), available at [http://www.madacenter.org/images/text_editor/annualrepE2017\(1\).pdf](http://www.madacenter.org/images/text_editor/annualrepE2017(1).pdf) (last visited 19 April 2019)
- OECD 'The economic impact of shutting down internet and mobile phone services in Egypt – OECD' (2019), available at <https://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm> (last visited 19 April 2019)
- Pangbur D 'An app for protecting kids online is growing popular with autocrats' Fast Company (2018), available at <https://www.fastcompany.com/40585513/an-app-for-protecting-kids-online-is-growing-popular-with-autocrats> (last visited 23 June 2019)
- Pearson J 'Canadian internet filtering company says it's stopped "alternative lifestyles" censorship' Vice (2019), available at https://www.vice.com/en_us/

- article/3kgznn/netsweeper-says-its-stopped-alternative-lifestyles-censorship (last visited 23 June 2019)
- Perloth N 'How spy tech firms let governments see everything on a smartphone' *Nytimes.com*. (2016), available at <https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html> (last visited 23 June 2019)
- Police Media Centre Archives (2019), available at <https://www.policemc.gov.bh/en-archives/?cat=important-telephone-number&type=month&year=2016&month=8&start=01/08/2016&end=31/08/2016> (last visited 23 June 2019)
- Privacy International 'The global surveillance industry' (2016), available at https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf (last visited 23 June 2019)
- Privacy International. 'Italy cancels surveillance export to Egypt but new undercover documentary shows surveillance industry brazenly continues to export to repressive regimes' (2017), available at <https://privacyinternational.org/advocacy-briefing/759/italy-cancels-surveillance-export-egypt-new-undercover-documentary-shows> (last visited 25 June 2019)
- Satter R 'AP NewsBreak: Undercover agents target cybersecurity watchdog' *AP NEWS* (2019), available at <https://www.apnews.com/9f31fa2aa72946c694555a5074fc9f42> (last visited 25 June 2019)
- Scott-Railton J et al 'Reckless VII: Wife of journalist slain in cartel-linked killing targeted with NSO group's spyware' - *The Citizen Lab* (2019), available at <https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/> (last visited 25 June 2019)
- Scott-Railton J et al 'Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware' - *The Citizen Lab* (2017), available at <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/> (last visited 25 June 2019)
- Seib P (2007) *New media and the new Middle East* Palgrave Macmillan
- Sonne P & Coker M 'Firms aided Libyan spies first look inside security unit shows how citizens were tracked' *Nytimes.com*. (2011), available at <https://www.wsj.com/articles/SB10001424053111904199404576538721260166388> (last visited 25 June 2019)
- Stahl L 'CEO of Israeli spyware-maker NSO on fighting terror, Khashoggi murder, and Saudi Arabia' *Cbsnews.com*. (2019), available at <https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/> (last visited 25 June 2019)
- Tesquet O 'Amesys: Egyptian trials and tribulations of a French digital arms dealer' *Telerama* (2017), available at <https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php> (last visited 25 June 2019)
- The Citizen Lab 'Planet Netsweeper executive summary' (2018), available at <https://citizenlab.ca/2018/04/planet-netsweeper/> (last visited 25 June 2019)
- The Citizen Lab 'The Citizen Lab: Research and development at the intersection of digital media, global security, and human rights' *Citizenlab.ca*. (2018), available at <https://citizenlab.ca/wp-content/uploads/2018/05/18033-Citizen-Lab-booklet-p-E.pdf> (last visited 25 June 2019)
- The Citizen Lab 'About the Citizen Lab - The Citizen Lab' (2019), available at <https://citizenlab.ca/about/> (last visited 25 June 2019)
- The Guardian* 'Any Palestinian is exposed to monitoring by the Israeli Big Brother' (2014), available at <https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-unit-testimonies> (last visited 25 June 2019)

- The Guardian* 'Israel expels 43 intelligence veterans who refused to spy in Palestinian territories' (2015), <https://www.theguardian.com/world/2015/jan/27/israel-expels-intelligence-veterans-who-refused-spy-occupied-palestinians> (last visited 25 June 2019)
- The International Federation for Human Rights 'The Amesys case' (2014), available at https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf (last visited 25 June 2019)
- Toor A 'Bahrain's internet shutdown marks a "new form of information control"' The Verge (2019) available at <https://www.theverge.com/2016/8/4/12373676/bahrain-internet-shutdown-duraz-protests> (last visited 18 April 2019)
- West DM 'Internet shutdowns cost countries \$2.4 billion last year' Brookings.edu (2016), available at <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf> (last visited 18 April 2019)
- Wikileaks *WikiLeaks - The spy files* (2011), available at https://wikileaks.org/spyfiles/docs/amesys/99_eagle-glnt-operator-manual-version-1-0.html (last visited 23 June 2019)

The impact of new information and communication technologies on the enjoyment of human rights in Latin America

Andrea Arriola,* Felipe Rivadeneira, Carlos Guzman,***
Mailen García**** and Claudio Nash*******

Abstract: *New information and communication technologies pose different and diverse challenges to the enjoyment of human rights in Latin America. This article presents a number of case studies on challenges and opportunities connected with ICTs and their impact on social movements, litigation, politics and the enjoyment of individual rights. It also refers to the attempts to promote the legal regulation of the digital sphere. The analysis highlights the gap between citizens with access to technology and connectivity and those left behind.*

Key words: *information and communication technologies (ICT); Latin America; legal regulation; digital rights; technology; connectivity; social inequality*

1 Introduction

Latin America is the most unequal region in the world (Kliksberg 2005). It is therefore unsurprising that new information and communication technologies (ICTs) have had a differential and potentially unequal impact in the enforcement of human rights in this region. Economic, geographical, age, sex, gender, linguistic, educational and cultural gaps – as well as those concerning employment and physical integrity – erode the equality of the populations of the region at the individual and collective levels, and have an impact on the possibility of access to and use of ICTs.

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. Master's in Human Rights and Democratization in Latin America and the Caribbean (LAT.MA); Lawyer; andrearriola@gmail.com

** Master's in Human Rights and Democratization in Latin America and the Caribbean Global Campus (LAT.MA); Lawyer; feliperivadeneira@hotmail.com

*** Master's in Human Rights and Democratization in Latin America and the Caribbean Global Campus (LAT.MA); Lawyer; caguzval@gmail.com

**** Master's in Human Rights and Democratization in Latin America and the Caribbean Global Campus (LAT.MA); Sociologist; garciamailena@gmail.com

***** PhD; Lecturer, Master's in Human Rights and Democratization in Latin America and the Caribbean (LAT.MA) and member of the LATMA Scientific Committee; claudionashrojas@gmail.com

The international community is committed to ensuring effective access to ICTs as reflected in the Sustainable Development Goals (SDGs). Despite this commitment and a certain decline in economic inequality in recent years in the region, can we consider that the digital gaps are the 'new inequalities' in the region? What are the differential impacts by age, gender, social class, ethnicity, physical integrity and place of residence, caused by new technologies?

Neither digital sovereignty nor the potentialities and risks of new technologies can be addressed without reference to the structural context influencing interactions in the region.

In Latin America, as elsewhere in the world, state authority to review digital content shared through the internet and the imposition of restrictions over its use should be in line with human rights and, in particular, with freedom of expression and conscience. In order to prevent illegitimate or arbitrary decisions, any limitations imposed must pursue a legitimate aim and must be proportional. Moreover, restrictions should have a basis in law and be set in advance, with citizen awareness of the purpose and limits of state control. State control cannot be intrusive and affect the right to privacy. Companies also play an essential role in ensuring this right. Legislation on data access and judicial review of these issues is essential.

Likewise, it is relevant to highlight the link between ICTs and human rights in different relevant social areas in Latin America, such as education, health and labour. In these respects, ICTs are tools providing a larger range of opportunities to fulfil and ensure these rights. Additionally, in a number of countries the development of social media applications has created new tools for denouncing human rights violations and facilitating access to information essential to victim assistance. However, it cannot be negated that ICTs pose challenges that have an impact on people's lives and their relationship with their environment in the countries in which they reside and throughout the region. The technological revolution has fostered a virtual context where both individuals who have and who do not have access to the internet face the violation of their fundamental rights.

In this context, a critical view of the potential violation of rights that occur in the internet and the problems related to it is called for. These include new forms of violence with transnational and massive impact and new challenges in terms of crime prevention. Prosecution and sanctions are additional challenges faced by states in light of the absence of appropriate regulations and clear jurisdictions as well as a collision between rights. Similarly, another issue to address is network anonymity. Although the principle of net neutrality is a guarantee for internet users, it may turn into an obstacle when investigating, prosecuting and punishing offenders.

In view of the above, it is clear that with the current technological revolution new challenges have emerged in the face of which states must provide an effective response in order to respect and ensure the human rights of all persons/users.

2 Latin America and ICTs

In Latin America the incorporation of technologies was initially associated with the idea of development. With the expansion of the internet, the issues associated with technologies focused on inclusion. The understanding that new technologies would enhance state capabilities to exchanges information and gain benefits that would facilitate the production of knowledge (Camacho 2005).

From a historical point of view, it is possible to distinguish technological gaps from digital divides. The first refer to the distance or the existing separation between the people who have access to or manage technology and those who do not; the second refer to the limitations in application of ICTs, meaning the distance between the people who know how to use them and those who do not (Santoyo & Martínez 2003). Although initially it was thought that the gaps would be overcome as the context improved, nowadays it is clear that those gaps persist, have been accentuated, and engender new forms of inequalities.

Since the World Summits on Information Society held in Geneva (2003) and Tunis (2005), Latin America has set for itself the objective of overcoming these gaps and the exclusion they bring to the populations lagging behind in the digital era (ECLAC 2017). For this region, the digital era is turning into a new phase of inequality not only related to technological inequalities but also to a manifestation of the social gaps (Arenas Ramiro 2011).

2.1 The gaps

When speaking of the digital divide we refer to a situation where countries lack the same opportunities to access the benefits of technologies, to have access to connectivity, and to be an active part of a network, not only within national boundaries but also regionally and globally. The United Nations Economic Commission for Latin America and the Caribbean (ECLAC) defines it as 'the dividing line between the population group that already has the possibility of benefiting from ICTs and the group that is still unable to do so' (ECLAC 2003: 16).

It is important to recognise the digital divide as a concept that, given its multidimensional and multifactorial nature, is in constant evolution and can generate different forms of inequalities. These include inequalities between countries (international digital divide) or between citizens within each country (internal digital divide), and these inequalities are generally accentuated between those who live in urban areas and those in rural areas (De la Selva 2015). When speaking about digital gaps, those relating to access, use, quality of use and technological appropriation must be taken into account.

Regarding access to ICTs and internet connection, 43,4 percent of all Latin American households were connected to the internet in 2015 (ECLAC 2016: 7). While in 2017 the percentage rose to 56 per cent, with the number of households growing by 103 per cent from 2010 to 2016, more than half the households still lacked access to the internet (ECLAC 2017).

As far as access to fixed broadband and mobile broadband is concerned, in 2010 the penetration of these was relative parity, by 6,5 per cent. It then is evident that the penetration of mobile broadband surpassed fixed penetration. In 2016 mobile broadband reached 64 per cent in relation to 11 per cent, corresponding to fixed broadband. However, mobile data traffic in the region continued to be the lowest in the world, with an average of 449 terabytes per month (ECLAC 2017).

The second type of gap relates to the ability to use ICTs and to navigate the network. It is necessary to point out that it is not enough to 'be online' if you do not know what information to look for in the network and how to identify a reliable source from one that is not. This skill is often associated with the educational level of the user, meaning that the users with high levels of education make better use of the information in the network. In Latin America, education depends on financial income available and social stratification. This will also to a large extent determine the quality of internet use, which is related to affordability and the speed of internet service.

One of the major challenges, particularly in Latin America, is the design and execution of projects aimed at digital literacy in order to effectively include all peoples, especially those belonging to populations in vulnerable situations (Camargo & Murillo 2012). In this regard, indigenous peoples are particularly affected by technology in their ancestral lands, mainly relating to extractive projects. These have brought violence against human rights defenders – some of which have lost their lives – defending ancestral lands against large private companies. An example on the use of ICTs for the benefit of indigenous communities is addressed below.

2.2 Digital gender gaps

An analysis of digital gender gaps as a consequence of asymmetric power relations involves the consideration of two elements: the dissimilarity between men and women in the use of ICTs, and that of women among themselves. In this sense, digital gender gaps must be analysed taking into account cross-cutting perspectives, meaning that access to the internet is not the same for a young professional woman living in the city, without disability, as for an older indigenous woman living in a rural community where connectivity quality and speed are not of an equal standard.

All contextual circumstances must be considered in order to understand structural inequalities in the region. These include unequal access to opportunities for women, as well as the gender stereotypes that historically have separated women from science and technology. In this sense, digital gaps are a consequence of pre-existing inequalities they generate or enhance new forms of exclusion.

In this context there are several examples of concrete actions developed to promote the incursion of girls in the world of science, mathematics and robotics, using technologies as key tools in the digital literacy process, with women/girls as creators, designers and producers of technologies.

Since 2016 Paraguay has promoted a project titled 'Girls Code', which seeks to awaken the interest of girls – in both public and private schools – in the use of technologies and inspire them in active participation through the development of skills and technical knowledge, as well as attitudes

aimed at making them feel capable of being the next generation of entrepreneurs, creators and change makers (Girls Code 2019). In order to achieve these objectives, the project carries out an active learning process through workshops and courses where girls self-pace their own learning processes, from being software consumers to software developers. These workshops provide basic notions about programming, the creation of web pages, applications for mobile phones, game design, handling of three-dimensional printers and the introduction to robotics. The workshops are held on weekends or after school, for girls from the ages of six to nine years and from ten to thirteen years. Many of the girls who participated in the workshops progress to more advanced courses, acquire confidence to share mixed spaces, and strengthen their ability to create and learn.

2.3 Digital gaps in technological appropriation

In order to address digital gaps – especially those connected with technological appropriation and the progression from technology consumers to technology developers for the benefit of the community – a number of good practices have been developed in different countries of the region.

In the Peruvian Amazon, indigenous peoples use ICTs to report oil spills in their river waters and pollution of their ancestral lands (Collyns 2018). They gather photographic evidence and record geo-referenced videos on their cell phones and drones to report oil spills and pollution, and call for state supervision and political support to monitor that the extractive companies operate under the framework of the law. Drones are also used by indigenous peoples in Colombia, Costa Rica, El Salvador, Guatemala, Honduras, México, Panamá (FAO 2016), among others in the region (UICN 2016).

Following the line of appropriation of ICTs, it is also worth mentioning the actions of Latin American governments focused on the development of the right to access information as essential in the governance modality. Thus, today open government is the way in which Latin American governments meet to ensure transparency in their efforts, participation and collaboration of citizens, with technological innovation being a cross-axis aimed at bringing people closer to state actions.

Several branches of government in the region have designed platforms enabling citizens to make online consultations, participate in activities, learn about the management, how much public officials earn, how the budget is executed of the institution, as well as access to services over the internet without having to go to the institution's headquarters, thus saving transportation costs and time.

2.4 Final thoughts

It is essential to use technologies as tools to access data, which could be transformed into information and then into knowledge. This access is key to decision making by holders of rights (citizens) and by institutions responsible for ensuring the respect, guarantee and fulfilment of those rights (states). It is also essential to identify the different types of digital gaps, the manner in which they impact on populations, and to design and implement strategies to overcome these gaps in order to ensure access to the benefits of ITC for all. Projects, programmes and initiatives on

empowerment, literacy and technological appropriation should aim to foster agile and inexpensive mechanisms to access fundamental rights, so as to contribute towards reversing inequalities in Latin American societies.

Public policies based on the principle of equality and non-discrimination are key to overcoming the gaps that reinforce the digital divide as its new face of inequalities in Latin America. These policies should strive towards quality access of technologies – that go beyond connectivity – at low cost, thus enabling accessibility and compressible capacities and contents, mainly using technology as a tool for the effective exercise of rights by individuals and communities.

3 Opportunities and challenges in the use of ICT in the area of economic, social and cultural rights

Latin America faces levels of inequality and poverty with a direct impact on the enjoyment of economic, social and cultural rights. This part will focus on the impact of ICTs either on the development of policies to ensure these rights or on the exacerbation of new types of breaches or challenges with special reference to education, health and labour.

3.1 Education

During the last two decades the implementation of ICT in the field of education has not been successful enough to achieve significant benefits for the Latin American region (UNESCO 2013). A first challenge has been the lack of sustainable policies and an adequate budget to make new devices available. A second challenge is the training of teachers in the area of ICT as a fundamental step towards the implementation of new technologies in the classroom (UNESCO 2013; Valdivia 2008). Additionally, traditional pedagogical models have not been designed in a manner conducive to the use of ICT. This creates challenges for the educational process of younger generations who are digital natives, because traditional models do not provide them with the opportunity to relate with tech devices in educational spaces (Valdivia 2008).

In response, some governments of the region have tried to implement a number of policies to improve digital accessibility and availability for populations facing socio-economic disadvantages, particularly in rural or marginal areas. One of the most successful experiences is the so-called CEIBAL – the Spanish acronym of ‘Educational Connectivity of Basic Informatics for On-Line Learning’ – Plan, established in 2007 to promote technological integration at the service of education to impulse processes of social inclusion and innovation and personal growth and reduce the access gap between the highest and lowest income quintiles (Plan Ceibal 2019).

Even though CEIBAL was only aimed at public education when it was first launched, after some years both public and private schools benefited from the programme. It included one laptop per student and wifi connectivity inside and outside of classrooms (Velasco 2011; Rivoir & Lamschtein 2012). The programme also provided students with equipment maintenance and repair (Plan Ceibal, 2019). The Plan has been supplemented with other projects such as Plan Ibirapitá, implemented in 2015 to promote the digital inclusion of low-income pensioners; Youth for

Programming, launched in 2017 in order to create new job opportunities for 1 000 17 to 26 year-olds by training them in programming. As a consequence, Plan CEIBAL is referred to as one of the most successful experiences in the implementation of ICT in education across populations in Latin America.

There have been other examples of innovative projects for education in the region, for instance through mobile and computer games. The Chilean game *Kokori* raises awareness on cell biology by defending human cells from the attacks of micro-organisms, so far with more than 60 000 downloads in 36 countries. *Qranio*, developed in Brazil, is a trivia interface where users answer a wide variety of questions relating to various categories with more than 12 million students registered (BID 2016).

Adaptive learning platforms – artificial intelligence-based software to understand learning needs and design personalised responses – are another strategy to be considered for the region (BID 2016; Smart Sparrow 2018). Two experiences worth mentioning are *Geekie* and the Latin-American implementation of *Aleks*. *Geekie* is a Brazilian platform aimed at providing training for university admission examinations through games and virtual tutorials. *Aleks* is a project developed by the McGraw Hill publishing house with Mexican universities, such as the UNAM and ITAM, and with a wide variety of universities in the United States. The system uses online evaluations to predict learning levels and adapt them to specific student needs (BID 2016).

3.2 Health

According to the Pan-American Health Organisation, it is estimated that 30 per cent of the population in the region lacks access to health services due to economic reasons, and 21 per cent gives up on looking for access because of geographical barriers (PAHO 2017). Additionally, the public spending in health measured as part of the gross domestic product (GDP) did not vary significantly between 1990 and 2007, with the exception of Cuba and Uruguay (Fernández & Oviedo 2010: 14). Recent data shows that only five countries – Canada (7,74 per cent); Costa Rica (5,65 per cent); Cuba (10,92 per cent); the United States (13,97 per cent) and Uruguay (6,5 per cent) – out of 34 countries of the Americas invest more than 5 per cent of their GDP in public health services (WHO 2016).

Advancements in ICTs in the area of health have been introduced at a slow pace despite their importance (Fernández & Oviedo 2010; 5G Americas 2016: 10). Additionally, the health sector currently faces two specific problems, namely, providing equitable access to quality services, and reducing or regulating the rising costs of these services (Rodrigues 2003). In this area, ICTs are particularly useful in a variety of processes such as monitoring the performance of health systems, electronic management of medical care procedures, logistical support for clinical work, and medical treatment of patients with chronic diseases or disabilities (Azevedo, Bouillón & Glassman 2011). Consequently, some governments or private research investigation groups have introduced the use of ICTs in specific programmes, with a variety of results.

One example of the implementation of ICT is the use of telehealth, involving telecommunications and virtual technology to deliver health care outside traditional healthcare facilities (WHO 2019), for example

through virtual health care or long distance professional assistance to obtain guidance in diagnosis, care and referral of patients. The use of the internet and mobile technologies is a fundamental part of the development of this type of remote help.

Especially during the last decade there have been several initiatives in the region to implement different forms of telehealth. Countries such as Brazil, Colombia, Venezuela, Mexico and Panama have implemented not only policies but also an adequate legal framework to promote teleservices. One relevant example is the programme of rural telemedicine in Panama, started in 2005. Another significant case is the Brazilian National Telehealth Programme, which started two years later and includes nine states and 900 cities. In the same year Colombia released a similar programme with a national scope (5G Americas 2016: 13).

ICT has been used to prevent unhealthy habits or to promote healthy practices with various results. Sex education programmes based on the use of the internet were offered at state schools in 21 Colombian cities. According to the research results, the majority of the participants experienced a significant improvement in knowledge and attitudes towards most of the topics taught. Among the topics were the prevention of sexually transmitted diseases (STDs); gender-based violence; and the use of condoms and other contraception methods (Azevedo, Bouillón & Glassman 2011: 135). The experience had positive results.

As far as the prevention of alcohol and drug consumption is concerned, the results were not positive enough. In Uruguay a programme was released for teenagers based on webpage access and text messages, but very few participants entered the website. Even though teenagers had raised awareness of the negative impacts of alcohol and drugs, most of them did not change their consumption habits. Researchers explained that the main cause for the disinterest in the website had been the non-structured and voluntary design of the whole programme (Azevedo, Bouillón & Glassman 2011: 136-137).

ICTs have been used for treating chronic diseases in the region. A negative experience can be also mentioned in Uruguay. In this country an experiment was developed with the main goal of helping patients with diabetes type II. The principal idea was to create a type of social network in order to access material for improving lifestyles and to interact with other patients. However, most of the participants did not enter the webpage, based on other variables such as civil status, age and education level (Azevedo, Bouillón & Glassman 2011: 138). In Peru, thanks to a video campaign directed at teenagers for the improvement of their blood iron levels, a significant majority visited healthcare centres to request iron pills (Azevedo, Bouillón & Glassman 2011: 139). In this sense, this campaign was aimed at reducing cases of poor nutrition and anaemia.

3.3 Labour

Thanks to the implementation of ICT, the labour sector has experienced a variety of consequences. On one hand, some studies have demonstrated that workplaces that have implemented ICT in their environments have created diverse necessities in the workforce (Chelala & Martínez-Zarzoso 2017: 154). In that way, companies have created new job opportunities, particularly in the higher and lower-skilled sectors (Dutz, Almeida &

Packard, 2018: 30-33). Also, the use of mobile applications – such as Glovo, Rappi, Uber, Cabify – have increased the dynamics of the economic sectors, but this has complicated the status of workers and their rights (Arreola 2019).

The major examples are two first instance judgments issued at the Autonomous City of Buenos Aires, Argentina. The first case refers to the massive dismissal by the company PedidosYa that affected 450 out of their 1 000 delivery workers, without any compensation. Labour attorneys state that delivery workers are bound by an employment relationship that is not fully recognised and protected by the company. Consequently, labour rights are not guaranteed in a context where there are no social security contributions, nor recognition of extra hours (McDougall 2019).

In the second case, companies that manage the applications Glovo, Rappi and PedidosYa – the three that offer delivery services in the country and, especially, in the capital city – were sued due to non-observance of traffic regulations. The delivery is made by bicycle, and most workers were not provided with health and safety accessories. Moreover, the companies failed to contract insurance against traffic accidents for its delivery workers who were expected to contract this themselves. For these reasons, the Court stated that it was necessary for companies to cover these costs, and that services should be suspended until regulations were complied with. It also found that companies must adopt appropriate measures to avoid workers' loss of profit during the suspension time (Iprofesional – Legal editorial staff 2019).

Both cases reflect the legal gaps in the protections for new forms of work relationships. Although in Argentina these problems are currently being reviewed by the judiciary, in the rest of the region these issues are still pending. Despite the creation of new income sources for many people across the region, regulations for this type of activities cannot only protect companies and production, but must also protect its workers who remain the most disadvantaged sector of the region.

3.4 Final thoughts

ICTs have provided an opportunity to understand new forms of protecting human rights, making education and health more accessible and available for different populational areas. In this way, some governments have potentiated its usefulness, and have developed important programmes aimed at satisfying the rights of marginal populations. Thanks to these policies, people who have traditionally been discriminated against have had the possibility of enjoying the benefits of ICT. Now, the challenge is that governments must maintain the sustainability of their projects and try to expand coverage to benefit wider groups.

However, in the work sector, ICT may be seen as a new possibility of reducing unemployment, but also as a new way of ignoring workers' rights. This is particularly serious in the region because ICT would start to create more breaches between those who are fully protected by law and those who are not. It is necessary for governments to consider this situation and to start legislating and to adopt adequate policies that avoid gaps and provide adequate protection to any kind of work relationship. In any of the cases, Latin America still needs to learn about the potentiality

that ICTs offer and applying them in diverse ways to human rights protection.

4 Social movements and ITC

When addressing ITCs and human rights in Latin America, some recent examples of social movements are relevant to the analysis, in particular those connected with the gender movement in Argentina and the anti-corruption movement in Guatemala.

4.1 Argentina's #8M #VivasNosQueremos

The feminist movement has gained momentum and it is spearheading in social change all around the world. In this context, the recent 'green' and 'purple' waves¹ are supported by hundreds of thousands of women in Argentina and have had an impact on social movements around the globe. Aside from its symbolism as 'international women's day', in Argentina 8 March – or #8M – has also become a reference for 8 October 2016.

In 2013 a wave of femicides, and the type of information available on these events, evidenced that there was no appropriate official data and statistics to understand and analyse the phenomenon. This led to the women's movement and civil society pushing for a debate on the issue. By 2015 the National Supreme Court's Gender Office reported that during that year 235 women were victims of femicide or gender-based violence (Registro Nacional de Femicidios de la Justicia Argentina 2015).

A number of high-profile femicides covered by the media at the time led civil society to implement a new communication strategy that was reproduced in multiple cities at the national level and abroad. This strategy included mass demonstrations, such as those carried out in connection with the so-called *miércoles negro*/Black Wednesday. *Miércoles negro* was organised in order to bring into focus the femicide of Lucía Pérez, a 16 year-old student brutally raped and killed by a gang of men.² Multiple protests and demonstrations were organised. Over a period of four months thousands of women participated in rallies and assemblies in 105 cities in a historic social protest for women's rights (Laudano & Kratje 2018). This gender-based violence case had a significant impact on Argentinian society.

In order to spread their message, the women's movement took advantage of new technologies and social media. A massive wave of communications were spread on Facebook, Twitter, YouTube and Vimeo (Laudano & Kratje 2018). Without social media platforms, the message against gender-based violence and the call for demonstrations would have not reached a massive audience in multiple locations. As indicated by Laudano and Kratje:

1 The women's movement in Argentina is currently identified by the colour green, representing support for sexual and reproductive rights; <https://www.infobae.com/cultura/2018/08/05/la-historia-del-panuelo-verde-como-surgio-el-emblema-del-nuevo-feminismo-en-argentina/> (last visited 10 April 2019).

2 See https://elpais.com/internacional/2016/10/19/argentina/1476905030_430567.html (last visited 10 April 2019).

In the communicational sense it was very important to recognize a poetical feeling linked to the audiovisual. For example, from the group *Ni una menos* the invitation to participate in the #8M march was addressed to women from different social levels and from different geographical origins, appealing to the breadth and diversity of values processed by a television aesthetic that uses the increasing speed of montage to transmit the urgency of the claim of #NiUnaMenos.

The social demonstrations against femicide promoted by the women's movement in Argentina was replicated in more than 70 countries, including Germany, Australia, England, France, Israel, Russia, Togo, Turkey and the rest of Latin America.

4.2 #RenunciaYa #JusticiaYa, the hashtags that made possible the removal of a President

Guatemala is located in the northern triangle of Central America and is considered the most unequal country in Latin America, with 0,53 points in the GINI index (ECLAC 2018). Between 1960 and 1996 Guatemala was devastated by a civil war that represents one of the darkest chapters in its political history, with more than 220 000 violent deaths and 45 000 disappearances (Historical Enlightenment Commission 1999). It was the first country in the world to request the support of the United Nations (UN) for the establishment of an international commission against impunity and illegal security forces and clandestine security gangs (Agreement between the United Nations and the Government of Guatemala regarding the establishment of an International Commission Against Impunity in Guatemala CICIG 2007).

In 2015 the country underwent a serious political crisis due to several investigations made by the CICIG. Those investigations revealed that former President Otto Perez Molina and former Vice-President Roxana Baldetti Elias were part of a criminal organisation involved in tax fraud³ and several more corruption cases.⁴ Civil society reacted with demonstrations in the central square of Guatemala City, called and organised under the hashtag #RenunciaYa.⁵ #RenunciaYa started like a collective call to show the government that the urban and middle-class were angered by the corruption cases.

As a response to calls made via Facebook, more than 40 000 people participated in the demonstrations.⁶ On 25 April 2015 thousands of Guatemalans demonstrated at the central park of Guatemala City, starting a cycle of protests that lasted for months until the resignation of Perez Molina and Baldetti Elias and their prosecution on corruption charges.⁷

3 See <https://www.mp.gob.gt/noticias/2017/10/27/caso-la-linea-juez-galvez-envia-a-debate-oral-y-publico-a-roxana-baldetti-y-otto-perez-molina-y-26-mas-implicados/> (last visited 10 April 2019).

4 See https://elpais.com/internacional/2018/10/10/america/1539127138_240195.htm (last visited 10 April 2019).

5 See <https://beersandpolitics.com/como-se-gesto-el-movimiento-renuncia-ya> (last visited 10 April 2019).

6 See <https://www.nytimes.com/es/2016/10/07/los-jovenes-que-aprendieron-a-hacer-politica-mientras-tumbaban-al-presidente-de-guatemala/> (last visited 19 April 2019).

7 See https://elpais.com/internacional/2015/06/14/actualidad/1434303266_370487.html (last visited 10 April 2019).

Some of the activists that organised the 2015 marches have gathered in a new social collective, popularly known as #JusticiaYa. This group is focused on battling corruption, inequality and the lack of transparency in Guatemala. As a backlash, some members of #JusticiaYa have been slandered and prosecuted as part of the challenges faced by social movements involved in the construction of a more inclusive and fair society.

4.3 The Xinka community and their campaign against open-pit mining

Guatemala's relations with the ITCs and the social movements did not end in Guatemala City and the mobilisations organised by the upper and middle urban class. The rural indigenous Xinka community is located in the south-east of Guatemala, 75 kilometres from Guatemala City in an area designated for a number of mining activities. The community is involved in an open fight against the government and Canadian mining companies due to the failure to comply with the right to a free, prior and informed consultation process with indigenous peoples in connection with the use and exploitation of ancestral lands.⁸ When the Xinka community brought the matter to the courts, it faced a 'media siege' by the mining company in order to block information on the case from the public.

With the purpose of sharing information on these cases with society at large, the community set up a communication strategy running in parallel with the court litigation. The communication strategy involved explaining the cases to social media influencers and inviting them to disseminate that information through their social media outlets; meetings with leaders of other indigenous communities facing the same challenges with mining activity and litigation; using the hashtag #YoSoyXinka on Twitter, Facebook and YouTube in order to make visible their cause; promoting demonstrations in Guatemala City to attract the attention of the mainstream media; calling for the demonstrations in social media in order to avoid the mainstream media siege; calling for demonstrations on the same day the hearings were held in court; and sharing short video recordings on Facebook in order to make them viral through the social networks.

Thanks to this communications strategy, the case brought before the Constitutional Court gained media profile and was well positioned in the national debate. Newspapers and television discussed the case of *San Rafael Las Flores v Mina El Escobal* (Quezada 2013). In its decision the Constitutional Court of Guatemala found that the state had failed to respect the right to a free, prior and informed consultation process with the Xinka community and that any processes to obtain a mining licence in the territory of indigenous peoples must be guided by the consultation standards. This case shows a clear strategy to avoid the media siege and place human rights cases on the national agenda (Cabrera 2012).

8 See <https://www.efe.com/efe/america/economia/la-corte-de-guatemala-ratifica-suspensi-on-una-minera-canadiense-y-ordena-consulta/20000011-3738309> (last visited 10 April 2019).

4.4 Final thoughts

Not every relationship between social movements and social networks builds or achieves positive change in society. In fact, there have been serious cases of criminalisation and defamation of social activists and human rights defenders through social media. Social media is also used to spread fake news during electoral processes or to destroy the image or reputation of candidates. It is undeniable that social networks are powerful tools to spread political messages.

5 The dilemma of legal regulation in Latin America

Since the 1996 Declaration of the Independence of Cyberspace,⁹ the neutrality of the Web and the willingness to remain exempt from any type of regulation have been a fundamental pillar. However, since 1993 Latin America has developed laws to try and regulate the possible crimes and harmful actions derived from the use of the internet. In this sense, Argentina was one of the pioneers with Law 11.723 of 1993, for the protection of copyright through the Internet. It also adopted Law 25.690 of 2003, regulating Internet providers. For its part, Brazil issued Law 9472 in 1997 regulating Internet service providers and issued Law 9610 in 1998 and Law 12270 in 2010 on the protection of copyright. Colombia with Law 1273 of 2009 and Mexico with the Federal Law on Transparency and Access to Government Public Information of 2002, have focused their legislation on the protection of personal data, in order to guarantee citizens' access to services and the security of their data.

Currently the region is debating the possibility of regulating publications on social networks (Facebook, Twitter and Instagram, among others), a question that is directly related to the limits on freedom of expression. However, it is not the only human right that could be violated. Social networks can be used to commit perjury and the right to a good name.

We will focus on three types of responses that different countries in the region have given on the possibility of regulating digital platforms, as a way to visualise from these latitudes how they are looking for answers to these new challenges.

Based on a study of both Bills and legislation in force in the region, three regulatory scenarios are discussed, namely, those of Colombia, Argentina and Ecuador: in the first place, an example where the judicial branch focuses on good practices; in the second place a Bill that, for political reasons, failed to prosper; finally, a 'negative' example in terms of freedom of expression where – due to a lack of political consensus – the legislation could not transcend the parliamentary sphere.¹⁰

9 See <https://www.eff.org/cyberspace-independence> (last visited 10 April 2019).

10 The case of Venezuela was debated in groups and it was decided not to include it in response to the complex situation the country is going through. On this occasion, it was decided to use the 'Ecuador' case as a similar reference model, even though the latter has not enacted legislation in this regard.

5.1 Colombia: Regulation by the judicial branch

The Constitutional Court of Colombia is the judicial entity responsible for ensuring the integrity and supremacy of the Colombian Constitution. This Court has received three complaints from citizens who resorted to the judicial recourse in cases of perjury and the right to a good name against them.

In the complaint the victims argue that these are crimes contemplated in the national law and that should not vary their possibility of trial because they occur online. Thus, the distinctive point in Colombia is that the possible solution could come from the judicial sphere rather than by new sanctioned legislation.

Nowadays the Constitutional Court of Colombia is studying the processes that seek the elimination of publications with libellous content as they are offences under national laws. During the last elections, there were insults among political candidates who attacked one another on social networks. Specifically, these were situations in which one person called the other a 'thief, swindler or corrupt' and the insults were disseminated through social networks with photos of the relevant individual, messages that are common to find when reviewing posts on Instagram or the Facebook wall.¹¹ This matter led to a public hearing on 28 February 2019. The hearing was organised as follows: first the parties and related parties (the three shareholders and the representatives of Google and Facebook); then the public authorities; and later on, the experts. The position of the representatives of the companies is that 'the administrators should not be responsible for the content made by third parties'. However, the Office of the Prosecutor of Colombia, represented by Néstor Humberto Martínez, argued that the right to freedom of expression was not absolute and when it comes into tension with other fundamental rights, '[t]here is a limitation in the expression that circulates in these highways of contemporary communication, they cannot serve as an instrument of apology to crime, they cannot serve to commit a crime'. Of course, the treatment of these matters 'cannot be a response from criminalisation' (Lorenzo Villegas Carrasquilla, Google LLC representative at the hearing).

During 2018 the Court gave eight judgments dealing with digital rights, the most relevant of these being the judgment that established that 'the guardianship judge may take measures against certain communications in a digital context always and when it is necessary to protect the right to good name and honour in specific cases' (T 121-2018).

5.2 Argentina: A good initiative with no end result

The case of Argentina represents a good initiative that failed to achieve parliamentary consideration because the political conditions to discuss such laws were not in place.

In our region, there are notable initiatives from civil society or some minority political sector that are made impossible due to unfavourable political conditions. Thus, in both the case of Argentina and Ecuador,

11 See <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/audiencia-sobre-redes-sociales-en-la-corte-constitucional-en-colombia-332412> (last visited 10 April 2019).

discussed below, the projects have not been approved and sanctioned by Parliament for political reasons exogenous to the initiatives.

In Argentina, the Bill¹² was promoted from the Senate by a member of the ruling coalition, Federico Pinedo (PRO), and by an opposition senator, Liliana Fellner (FPV) and obtained a half sanction. However, it was not dealt with by the Chamber of Deputies. In addition, the initiative has the support of the UN and OAS freedom of expression rapporteurs and the internet industry in Argentina, the telecommunications industry and various civil society organisations. The experts considered that it was a good Bill of responsibility of intermediaries on the internet as it states that 'intermediaries are not responsible for the contents that users upload or circulate through their platforms or services, except when they do not comply with a court order that obliges them to do so' (Project Bill number S-1865/15 y S-942/16, 2016).

Among the organisations that publicly expressed their support are Access Now; Ageia Densi; Centre for Technology and Society Studies, University of San Andrés; Datas; Faro Digital; Via Libre Foundation; and Public Knowledge. In a public letter they argue (AAVV 2017):

Intermediaries play a crucial role in the exercise of fundamental rights on the internet and, therefore, citizens must be protected from any regulation that denatures their function and grants them the authority to remove content that is exclusive to the judiciary. It should never be the private sector responsible for resolving the legality or not of the information published by an internet user.

Among the detractors of the initiative are associations that protect copyright. The Argentine Chamber of Books (CAL), the Argentine Chamber of Publications (CAP), the Reprographic Rights Administration Centre (CADRA), and the Argentine Chamber of Producers of Phonograms and Videograms (Capif). These organisations argued that the initiative eliminates the responsibility of the service providers and that, therefore, the platforms could not download content protected by copyright without a court order.

5.3 Ecuador: Challenges to freedom of expression

The last example to analyse the situation in Latin America is the Ecuadorian case, which stands out for its errors in design, analysis and implementation. In short, Ecuador is the negative example in our region.

A day before leaving the presidency, Rafael Correa sent to the National Assembly a Bill to regulate acts of hatred and discrimination on social networks and the internet. The Bill included a provision placing an obligation on social network service providers to submit quarterly reports on claims of illegal content received from users and the actions and their own actions to prevent criminal acts. It also established a series of fines and penalties for companies that do not comply (Correa 2017).¹³

12 The Bill is available at <https://drive.google.com/file/d/1EO1As7v0PNrTirzAK5o0e2x83jklQ0I9/view> (last visited 10 April 2019).

13 See <https://www.eluniverso.com/noticias/2017/05/25/nota/6199663/proyecto-rafael-correa-regular-redes-sociales-llego-asamblea> (last visited 10 April 2019).

Both in 2018 and 2019, PAIS Alliance Assemblyman Daniel Mendoza presented a draft Organic Law of Responsible Use of Social Networks.¹⁴ Its objective was to engage users in the use of networks and expressly prohibit the dissemination of fake news, hate messages or information that could compromise third parties or put national stability at risk. It provides for a penalty of one to three years in prison (Bill No. 356924). However, the project does not have the support of the other political sectors in Ecuador. It has been argued that the Bill does not conform to international standards and that it violates freedom of expression. Mendoza said in an interview with the newspaper *El Comercio* that his Bill was different from that of Correa since it does not seek to censor freedom of expression, as allegedly the former President's did, but rather to regulate the platforms.¹⁵

5.4 Final thoughts

The examples above include different strategies developed in Latin America to move forward in a complex and current challenge: Colombia seems to move forward while Argentina has failed to do so due to the lack of a broader political agreement, and Ecuador has for the moment avoided a restrictive model of regulation due to the change of government and a failed parliamentary initiative.

6 Conclusion

Latin America must focus on eradicating social inequalities. ICTs could be an instrument to contribute to that eradication, or it may become an instrument to reproduce those inequalities and increase the gap between new categories of Latin-American citizens: those integrated into the digital world and those excluded from it. For the human rights movement this is an area of concern. A failure to integrate communities into the digital age may prove to be too difficult to revert. There are some positive, mostly isolated, examples. Progress requires change. It is not clear whether states, the private sector or civil society will be the main engines of this required change.

References

- 5G Americas Telehealth in Latin America 2016. 5G Americas (2016), available at http://www.5gamericas.org/files/6814/7190/3108/WP_TeleHealth_English_Final.pdf (last visited 10 April 2019)
- AAVV Organizaciones argentinas apoyan proyecto de intermediarios en Internet. *Via Libre* 17 de noviembre de 2017, available at <https://www.vialibre.org.ar/>

14 See <https://observatoriolegislativocele.com/wp-content/uploads/Ecuador-Proyecto-de-Ley-del-Uso-Responsable-de-Redes-Sociales-2019.pdf> (last visited 10 April 2019).

15 See <https://www.elcomercio.com/actualidad/daniel-mendoza-ley-redes-sociales.html> (last visited 10 April 2019).

- 2017/11/17/organizaciones-argentinas-apoyan-proyecto-de-intermediarios-en-internet/ (last visited 10 April 2019)
- Agenda de la audiencia: Libertad de expresión en el uso de redes sociales 29 de febrero de 2019. *Noticias de la Corte Constitucional de Colombia*, available at <http://www.corteconstitucional.gov.co/noticia.php?Agenda-de-audiencia-Libertad-de-expresion-en-el-uso-de-redes-sociales.-8700> (last visited 10 April 2019)
- Arenas M (2011) 'Brecha digital de género: la mujer y las nuevas tecnologías' Anuario de la Facultad de Derecho: Universidad de Alcalá
- Arreola G (2019) 'No son las aplicaciones, tampoco los taxistas, es la precarización'. CISS - Conferencia Interamericana de Seguridad Social, available: <https://ciss-bienestar.org/wp-content/uploads/2019/06/No-son-las-aplicaciones.pdf>
- Azevedo V, Bouillón C & Glassman A (2011) 'Fiebre tecnológica en el sector salud' in A Chong (ed) *Conexiones del desarrollo. Impacto de las nuevas tecnologías de la información* Washington DC: Fondo de Cultura Económica 123-156
- Bécares B (2016) 'La brecha digital persiste en América Latina', available at <https://www.siliconweek.com/e-regulation/la-brecha-digital-persiste-en-america-latina-64840> (last visited 10 April 2019)
- BID (2016) *Graduate XXI. Un mapa del futuro. Cincuenta innovaciones educativas en América Latina* Washington DC: BID
- Cabrera, E M (2012) *Biblioteca Universidad de San Carlos de Guatemala*. Obtenido de Análisis comunicacional de campaña social realizada por el Centro de Acción Legal Ambiental y Social de Guatemala (CALAS) en el año 2010: http://biblio.teca.usac.edu.gt/tesis/16/16_0910.pdf (last visited 10 April 2019)
- Camacho K 'La brecha digital. Palabras en juego: enfoques multiculturales sobre las sociedades de la información' (2005), available at <https://vecam.org/archives/article550.html> (last visited 10 April 2019)
- Camargo DRB (2012) *El acceso de los pueblos indígenas a las tecnologías de la información y la comunicación en Colombia: ¿inclusión o exclusión social y política?* Derecho y Realidad Núm. 20, Segundo semestre de 2012 Facultad de Derecho y Ciencias Sociales. Universidad Pedagógica y Tecnológica de Colombia
- Carrión C (2017) *Ley de control a redes sociales última mordaza contra la libertad de expresión*. Blog de la Asamblea Nacional de Ecuador), available at <https://www.asambleanacional.gob.ec/es/blogs/cesar-carrión/52055-ley-de-control-redes-sociales-ultima-mordaza> (last visited 10 April 2019)
- Castilla J 'Siga en vivo la audiencia de la Corte Constitucional sobre el uso y control de las redes sociales' *Asuntos legales* (2019), available at <https://www.asuntoslegales.com.co/actualidad/inicia-en-la-corte-constitucional-audiencia-sobre-el-uso-y-control-de-las-redes-sociales-2833912> (last visited 10 April 2019)
- CEPAL *Los caminos hacia una sociedad de la información en América Latina y el Caribe* (2003), available at <https://www.cepal.org/es/publicaciones/2354-caminos-sociedad-la-informacion-america-latina-caribe> (last visited 10 April 2019)
- CEPAL *Ciencia, tecnología e innovación en la economía digital. La situación de América Latina y el Caribe*. Segunda Reunión de la Conferencia de Ciencia, Innovación y TIC de la CEPAL (2016), available at https://repositorio.cepal.org/bitstream/handle/11362/40530/3/S1600833_es.pdf (last visited 10 April 2019)

- CEPAL *Estado de la Banda Ancha en América Latina y el Caribe* (2017), available at https://repositorio.cepal.org/bitstream/handle/11362/43365/1/S1800083_es.pdf (last visited 10 April 2019)
- CEPAL (2018) *Social Panorama of Latin America* Santiago de Chile: United Nations
- CEPAL (2019) *La Autonomía de las Mujeres en Escenarios Económicos Cambiantes* Santiago
- Chelala, S & Martínez-Zarzoso, I (2017) '¿Sesgo anti-innovación? El impacto tecnológico de los acuerdos comerciales' in *Robotlución, El futuro del trabajo de la integración 4.0 de América Latina*
- Collins, D (2018) 'Petróleo en el agua: el uso de la tecnología para luchar contra un legado tóxico'. MONGABAY, available at <https://es.mongabay.com/2018/02/petroleo-en-el-agua-drones/> (last visited 10 April 2019)
- Davidovsky S 'Cómo es el proyecto de ley que busca regular la responsabilidad de los intermediarios en Internet' *La Nación* (24 November 2017), available at <https://www.lanacion.com.ar/tecnologia/como-es-el-proyecto-de-la-ley-que-busca-regular-la-responsabilidad-de-los-intermediarios-en-internet-nid2084998> (last visited 10 April 2019)
- De la Selva ARA 'Los nuevos rostros de la desigualdad en el siglo XXI: la brecha digital' (2015) 60 *Revista mexicana de ciencias políticas y sociales* 265
- Dutz M, Almeida R & Packard T (2018). *The jobs of tomorrow – Technology, productivity, and prosperity in Latin America and the Caribbean* Washington: World Bank
- FAO (2016) 'Comunidades de Mesoamérica mejoran herramientas para manejar sus bosques', available at: <http://www.fao.org/panama/noticias/detail-events/zh/c/433504/>
- FAO (2016) 'Indígenas de Panamá se capacitan en uso de drones para cuidar el bosque', available at: <http://www.fao.org/americas/noticias/ver/es/c/417512/>
- Fernández A & Oviedo E (2010) *Tecnologías de la información y la comunicación en sector salud: oportunidades y desafíos para reducir inequidades en América Latina y el Caribe*. Santiago de Chile: ONU - CEPAL
- García García M & López Azuaga R 'Explorando, desde una perspectiva inclusiva, el uso de las TIC para atender a la diversidad' (2012) 16 *Revista de curriculum y formación del profesorado*
- Girls Code (2019) available at: <https://www.girlscode.com.py/> (last visited 10 April 2019)
- Historical Enlightenment Commission (1999) *Guatemala, memory of silence*. Guatemala City: United Nations service office for projects
- Horizontes Cepal Capítulo 9: Entrevista a Laís Abramo (2017), available at <https://www.cepal.org/es/videos/horizontes-cepal-capitulo-9-entrevista-lais-abramo> (last visited 10 April 2019)
- Jara Valdivia I (2008) *Las políticas de tecnologías para las escuelas en América Latina y el mundo: visiones y lecciones* Santiago de Chile: CEPAL
- Klikhsberg, B 'América Latina: La región más desigual de todas' (2005) 11(3) *Revista de Ciencias Sociales* 411-421, available http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1315-95182005000300002&lng=es&tlng=es.
- Laudano C & Kratje J Facultad de Humanidades y Ciencias de la Educación, Universidad de La Plata. *Memoria académica. Compartimos lo que sabemos* (2018) 379, available at http://www.memoria.fahce.unlp.edu.ar/art_revistas/pr.9028/pr.9028.pdf (last visited 10 April 2019)

- McDougall F PedidosYa, día después: prevén juicios masivos a las delivery y extensión de la responsabilidad a los comercios iProUp, available at <https://www.iproup.com/economia-digital/3072-dash-ico-plataforma-PedidosYaRappiGlovo-en-juicio-laboral-responde-el-comercio> (last visited 26 April 2019)
- Muro V 'La discusión por la responsabilidad de intermediarios en Internet podría volver' *La Nación* 8 November 2018, available at <https://www.lanacion.com.ar/tecnologia/la-discusion-responsabilidad-intermediarios-internet-podria-volver-nid2189718> (last visited 10 April 2019)
- OPS-PAHO Salud en las Américas (2017) Washington: OPS-OMS. Obtenido de, available at https://www.paho.org/salud-en-las-americas-2017/?post_type=post_t_es&p=290&lang=es (last visited 10 April 2019)
- Payán S 'Tres conclusiones inesperadas de la audiencia sobre libertad de expresión y redes' (5 March 2019) *Cero setenta*, available at <https://cerosetenta.unian.edu.co/tres-conclusiones-inesperadas-de-la-audiencia-sobre-libertad-de-expresion-y-redes/> (last visited 10 April 2019)
- Plan Ceibal 'What is Plan Ceibal', available at <https://www.ceibal.edu.uy/en/institucional> (last visited 29 April 2019)
- Quezada, R B *Plaza Pública*, 16 September 2013 available at: <https://www.plazapublica.com.gt/content/el-pico-del-conflicto-minero>
- Rivoir A & Lamschtein S (2012) *Cinco años del Plan Ceibal* Montevideo: UNICEF
- Rodrigues R 'eHealth in Latin America and the Caribbean: Development and policy issues' (2003) *Journal of Medical Internet Research*, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550550/> (last visited 21 April 2019)
- Santoyo AS & Martínez EM (2003) *La brecha digital: mitos y realidades*. Uabc
- Smart Sparrow 'Let's talk about adaptive learning' (2018), available at <https://www.smartsparrow.com/what-is-adaptive-learning/> (last visited 25 April 2019)
- UICN (2016) 'Nuevo mapa muestra cómo los pueblos indígenas de Centroamérica ocupan y resguardan gran cantidad de bosques, ríos y aguas costeras'. available at: <https://www.iucn.org/es/content/nuevo-mapa-muestra-como-los-pueblos-indigenas-de-centroamerica-ocupan-y-resguardan-gran-cantidad-de-bosques-y-aguas-costeras>
- UNESCO (2013) *Enfoques estratégicos sobre las TICS en educación en América Latina y el Caribe* Santiago de Chile: UNESCO
- Velasco C 'Plan Ceibal (II), más que 'un ordenador por niño'. *wwwwhat's new*, available at <https://www.whatsnew.com/2011/10/17/plan-ceibal-ii-mas-que-un-ordenador-por-nino%E2%80%9D/> (last visited 10 April 2019)
- WHO Global Health Expenditure Database – NHA Indicators (2016), available at <https://apps.who.int/nha/database/ViewData/Indicators/en> (last visited 28 April 2019)
- WHO Health and sustainable development – Telehealth (2019), available at <https://www.who.int/sustainable-development/health-sector/strategies/telehealth/en/> (last visited 28 April 2019)

Dystopia is now: Digital authoritarianism and human rights in Asia

Mark Anthony V Ambay III,* Neha Gauchan,**
Mahesti Hasanah*** and Numfon K Jaiwong****

Abstract: The advent of new information and communication technologies has opened up new economic opportunities, heightened the availability of information, and expanded access to education and health knowledge and services. These technologies have also provided new avenues for political, economic, social participation, and have presented new opportunities and methods for the advancement of human rights. At the same time, these same technologies can be used to violate human rights. This article queries as to how exactly states and other actors use digital authoritarianism to limit human rights. The study aims to understand what threats to human rights are presented by using new information and communication technologies. The article critically examines available literature on authoritarian practices using information and communication technologies, reports of government and intergovernmental bodies, non-governmental organisations, and various media agencies as well as by gathering first-hand data of samples of digital authoritarianism. The article argues that states and other actors practise digital authoritarianism by invading privacy, denying access to information and spreading misinformation, and limiting expression and participation, all of which violate the rights to freedom of expression, information and participation. Case studies of digital authoritarian practices are presented in the study, drawing on experiences and circumstances in several Asian countries.

Key words: digital authoritarianism; authoritarian practices; human rights; Asia; information and communication technology

1 Introduction

Every move you make is watched by millions of cameras, recorders and applications around you, even inside your own home. You wish to contact your family and friends but the network is down. You go online to read the news on what is happening, but your screen says 'HTTP 404'. You post #WhatIsHappening on your social media account but the post does not go through. A few hours later, security officers knock on your door to take you away. You are never heard again.

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. MA (Human Rights and Democratisation); Programme Manager, Global Campus of Human Rights Asia Pacific; ihrpmhrd@mahidol.edu

** MA (Human Rights and Democratisation); Researcher, ChildSafeNet Nepal, neha.gauchan.96@gmail.com

*** MA (Human Rights and Democratisation); Researcher, Research Centre for Politics and Government, Universitas Gadjah Mada; mahesti.hasanah@mail.ugm.ac.id

**** MA (Human Rights and Democratisation); fonjaiwong@gmail.com

While the situation sounds like it is straight out of a dystopian, futuristic science fiction film, it is not. It is happening, today, in nearly all countries. New information and communication technologies (ICTs) can help bridge social and economic inequalities by opening up new economic opportunities and helping to uplift countless millions from poverty, heightening the availability of information necessary for better policy and decision making, and expanding access to education and health services. These new ways of obtaining and exchanging information and communication with other people have also provided new avenues for political, economic and social participation. Advocacy groups, in particular, are successfully making use of these ICTs, especially the internet, in working for human rights, democracy and peace in even the most closed-off, authoritarian countries.

Yet, these same ICTs must also be viewed as a double-edged sword. Political actors, particularly governments, recognise the potential of ICTs, and many repressive regimes have subsequently developed new ways of limiting human rights and democracy using ICTs in a phenomenon that the advocacy group Freedom House has dubbed the 'rise of digital authoritarianism' (Freedom House 2018). Hence, this study explores how exactly states and other actors use digital authoritarianism to limit human rights.

This article aims to better understand the threats to human rights by using new ICTs. It seeks to identify the various ways in which states and other vested actors are using ICTs to limit access to and the exchange of information and communications to stifle opposition and dissent. The article critically examines relevant literature, reports of governments and intergovernmental bodies, non-governmental organisations (NGOs) and various media agencies as well as by gathering first-hand data of samples of digital authoritarianism, the article argues that states and other actors practise digital authoritarianism by invading privacy, denying access to information and spreading misinformation, and limiting expression and participation, all of which violate the rights to freedom of expression, information and participation. After reviewing research on the current status of digital authoritarianism. The article illustrates how digital authoritarianism is practised specifically in the Asian Pacific.

2 Authoritarianism in the digital sphere

The world is currently experiencing a 'global turn to authoritarianism' (Murakami Wood 2017: 358). This trend threatens to reverse the gains made by human rights movements in the last several decades. It is important to study how authoritarianism, in all its forms, affects human rights in order to better defend human rights against it. Political studies at one point or another invariably refer to Spanish political scientist Juan Linz in defining authoritarianism. Linz (2000: 159) saw authoritarianism as a political system that has limited political pluralism, lacks a guiding ideology but with a distinctive mentality, with the limited or minimal political mobilization of and participation by the populace, and ill-defined powers of the leaders.

It is not surprising to hear that under the presidency of Xi Jinping, 'China appears more authoritarian, not less' (Ang 2018) or that there is 'a

deepening of authoritarian rule' in Thailand (Mérieau 2018). However, in supposedly democratic countries in Asia, where elections are regularly held and civil and political liberties are supposedly guaranteed by law, commentators consider that 'an authoritarian India has emerged' (Nilsen 2018) and that 'the Philippines just became more authoritarian' (Santos 2019). It seems that, currently, Linz's definition of authoritarianism no longer is as clear-cut as before.

International relations scholar Glasius (2018) suggests that instead of focusing on authoritarian regimes or leaders, the study should be one of the authoritarian practices, thus allowing an analysis of the actions of political actors once they are in power. This goes beyond state-centric or single-state analyses of authoritarianism to explore settings that transcend state boundaries, and identify and interrogate the involvement of both state and non-state actors involved in authoritarianism.

This suggestion also means that authoritarian practices can be analysed in even so-called democratic countries, where the classic definitions of authoritarianism do not apply. The study of authoritarian practices can also be utilised in analysing how ICT is being used to suppress rights and freedoms through arbitrary surveillance, secrecy and disinformation, and the violation of freedom of expression (Glasius & Michaelsen 2018).

Japanese sociologist Yoneji Masuda (1980) argues that the advent of new information and communication technologies, most especially the internet, and the post-industrial 'information age' will usher in a new era of participatory democracy and democratisation, the emergence of 'information communities', and a spirit of globalism. Indeed, at least to a certain extent and for those who can avail of these new ICTs, the storage, access, and exchange of information and communication are faster and more reliable. New economic opportunities and modes of working have opened up, learning and training has become easier, and work processes are becoming more digitised and automated.

ICT has also presented new opportunities for the advancement of human rights. Social media and messaging applications such as WhatsApp have been utilised to mobilise people in defending their rights and interests (Breuer 2012; Ruijgrok 2016; Smidi & Shahin 2017). The internet plays an important role in assisting human rights organisations to gather and disseminate information about human rights to the general populace (Halpin & Hick 2000). New information storage systems make it easier to store and transport information. Even the ordinary smartphone can be a powerful tool to record and document human rights violations.

This technology, however, is a double-edged sword. Authoritarian practices in the digital sphere using ICTs are also used to restrict and violate human rights (Michaelsen & Glasius 2018). Privacy is invaded when a person's actions are continuously monitored by state-of-the-art surveillance systems, with all the data stored in a database accessible to state security forces at any given time (Lucas & Feng 2018). Internet access is restricted – or even suspended – to limit access to information that may have a bearing on social and political issues (OpenNet Initiative 2013). Shutdowns of telecommunication services are also used to prevent communications between political dissenters and to stop political mobilisation, whether spontaneous or organised (Wagner 2018).

Contrary to popular belief, these situations occur in both repressive and democratic countries, as evidenced by Hintz and Milan's study on the use of ICT for the surveillance and monitoring of citizens by governments in the 'liberal West' (Hintz & Milan 2018). Another example would be the use of social media in manipulating public opinion through employing fake social media accounts to support the candidacy of Donald Trump when he was running for President of the United States (Mayer 2018). In this regard, Freedom House (2018) refers in its report to the 'rise of digital authoritarianism'.¹

3 Defining digital authoritarianism

Before attempting to define digital authoritarianism as a concept, it is important to acknowledge that this article builds on the definition of authoritarian practices by Michaelsen and Glasius (2018). In their essay they introduce the twin concepts of illiberal and authoritarian practices. The former, they argue, infringes on the 'autonomy and dignity of a person' (Michaelsen & Glasius 2018: 3797). As such, it is a human rights issue. The latter, on the other hand, sabotages accountability, thereby threatening democratic processes and therefore is a democracy problem (Michaelsen & Glasius 2018: 3797).

Michaelsen and Glasius (2018: 3796) argue that threats to people in the digital sphere can be arranged into three categories: arbitrary surveillance; secrecy and disinformation; and violations of freedom of expression or disabling voice. While arbitrary surveillance is an illiberal practice and, therefore, a human rights violation, secrecy and information are authoritarian practices as it sabotages the accountability of leaders to their constituents. Violations of freedom of expression, they argue, are both illiberal and authoritarian practices (Michaelsen & Glasius 2018: 3804). This is where this article diverges from Michaelsen and Glasius. All three above-mentioned categories are human rights issues and lead to human rights abuses in the digital sphere. Each of these three categories violates specific human rights, as laid out in the major Covenants. Arbitrary surveillance violates one's right to privacy while secrecy and disinformation go against the right to information. The third category is stated as a violation of freedom of expression, but it is also a violation of the right to participation, and the right to be involved in political and public affairs. Thus, with regard to this article, it matters little whether the three categories mentioned by Michaelsen and Glasius affect the individual or sabotage accountability. What is clear is that they violate universally-recognised human rights. They are, therefore, human rights issues.

With this in mind, we define digital authoritarianism as practices using information and communication technology designed to either invade privacy, deny access to information, spread misinformation, limit expression, and limit political participation.

¹ The report lacks a precise definition of what exactly digital authoritarianism constitutes. Despite this weakness, the report is useful in assessing current trends on the use of new ICTs in suppressing freedoms and rights.

4 (Digital authoritarian) practice makes perfect

In an effort to control information and communications, several Asian governments engage in digital authoritarianism, often in cooperation with government-controlled or private companies that provide information and communication technology and services. These efforts are usually backed up by draconian laws and policies that allow governments to control the ingress and outflow of information and communications where they deem fit. There are at least 29 laws and policies in 15 countries in the region that give governments the authority to access personal data, shut down communications, and limit or block information exchange, with no mechanisms available to appeal. Other countries, while not having specific policies governing information and communication, have established regulatory bodies with sweeping powers that often have little oversight and accountability. In many countries there are both regulatory bodies and the laws that empower them. National security or public safety is frequently used as a justification. However, in many instances, curbing public discontent is the underlying reason, as the examples in this part will show.

5 Invasion of privacy: Surveillance and censorship

In the past two decades Asian governments have been using technical and legal strategies to regulate online content. A confluence of technology, behavioural science and market power has been used to increase internet surveillance and censorship in many countries (Clark et al 2017). The best example is China where authorities restrict access of citizens to information, searches and applications available on the internet. Since 2018, all the internet and application providers, such as Alibaba, Baidu, Byte Dance and Tencent, are required to keep a log with information such as activities of users posting on blogs, chat rooms, short video platforms and webcasts, which the authorities can monitor or access at any time. This ruling is aimed at preventing online users from engaging in activities that would potentially influence public opinion. In April 2018, Chinese authorities ordered Byte Dance to shut down a popular social media platform where users often shared jokes, videos and GIFs, which the governments regarded as displaying improper public opinion. Later, in December 2018, Reuters reported that China has closed 1 100 social media accounts and 31 websites that it accused of unlawful activities such as trolling or blackmail (Meyer 2018).

All internet or application providers in China are Chinese companies as foreign internet sites and applications are censored and blocked. Chinese companies are required to log information for authorities to monitor at any time, giving the government absolute power to monitor its digital space. China recently developed a new high-technology surveillance system scoring its citizens, called 'social credit'. This ranking of social credit will monitor the behaviour of China's enormous population. The social credit system, which was first announced in 2014 and is due to be fully operational nationwide by 2020, is currently being piloted for millions of people across the country. A person's social score can move up and down depending on their behaviour, such as bad driving, smoking in non-smoking zones, purchasing too many video games, and posting fake

news online (Ma 2018). A high social score means that they will receive a variety of privileges, such as discounted energy bills and the ability to forgo deposits on car and rental properties. In addition, they might get better treatment at Chinese hospitals (Marr 2019). However, as far as those with low scores are concerned, China has already started punishing people by restricting their travel. *Channel News Asia* (cited by Ma 2018) reported in March that over nine million people with low scores have been blocked from buying tickets for domestic flights. Furthermore, the government can ban them or their children from enrolling in the best schools. *Beijing News* reported that 17 people who had refused to do military service were barred from enrolling for higher education, applying for high school, or continuing their studies (Xueying 2018). Individuals would also be banned from managerial employment in state-owned firms and large banks, as well as being publicly named bad citizens. The scores are to be monitored by high-technology surveillance cameras. Across China more than 200 million cameras will be equipped with facilities for facial recognition, body scanning, and geo-tracking in order to keep a constant vigil over every citizen.

China is not the only country that aims to use this high-technology surveillance system. Chinese surveillance and security start-up technology has made its foray into Malaysia, by the supply of wearable cameras with artificial intelligence-powered facial recognition technology to local law enforcement agencies (Tan 2018). In January 2018 the Chinese company Yitu opened its first overseas office in Singapore to serve Southeast Asia, Hong Kong, Macau and Oceania. The Yitu technology can identify a person from its database of 1.8 billion people within three seconds with an accuracy of 95 per cent. This technology is being used in public spaces such as airports, banks and hospitals in China (Tan 2018). Investment in AI in the Asia-Pacific region has grown in prominence as governments seek to adopt technologies for urban management. This has raised concerns over the privacy of an individual and their basic fundamental rights.

6 Misinformation and the right to information

6.1 Fake news and misinformation

States have jumped into cyberspace to create and present their information, but in many cases this is not representing factual information. For example, India, where Facebook users exceed 300 million, experienced violence incited by falsities about child abductions spread mostly via social media. WhatsApp and other social networks led to 24 deaths from mob violence (Fernandez 2019). Scores of people across the country were lynched by mobs that suspected them of being child kidnappers (Jain 2018). Unfortunately the incidence of child kidnapping is increasing, so the fake news and disinformation in this case has allowed the actual child traffickers to continue as they are not spotted by mobs.

In Thailand the military junta filed charges against Thanathorn Juangroongruangkit, the leader of the Future Forward Party (FFP), for spreading fake information under the Computer Crimes Act. Thanathorn argued that the law was used to silence and threaten opposition (Fernandez 2019). The FFP was one of the main opposition parties to the

National Council for Peace and Order (NCPO) to the Thai junta during the general election in the early of 2019. The NCPO filed a complaint with the Technology Crime Suppression Division (TCSD) against Thanathorn and two other members of FFP for feeding false information into a computer system. The NCPO claimed that Thanathorn had used his personal Facebook and Party Facebook pages to accuse the NCPO of luring former members of parliament to back the regime by using existing lawsuits against them as a bargaining chip. Thanathorn told reporters that 'the Computer Crimes Act is used to silence and threaten us and to create politics of fear in this country' (*Bangkok Post* 2018). These allegations have raised concerns that the new regulations are enabling the corrupt government to stifle political rivals and free speech in Thailand.

6.2 Hate speech, racism, discrimination

In 2014 the Minorities Rights Group International published *State of the world's minorities and indigenous peoples*, presenting case studies of 70 countries across the globe, ranking these based on the dangers of hate speech and discrimination faced by minorities. Three Asian countries, Myanmar, Afghanistan and Pakistan, are ranked in the top ten. Hate crime by definition is any crime committed as a result of hostility towards someone because of their race, ethnicity, religious beliefs, disability or sexual orientation (Anwar 2014). In Myanmar, the government continues to circulate misinformation about the Rohingya Muslims. Facebook was used by the Myanmar government to spread disinformation about tensions between its citizens to incite violence against the Rohingya people (Brown 2019). Violence has spread to other parts of the country, where the killing of Muslims has been carried out by local mobs or Buddhist groups (Seiff 2014). Discriminatory violence in Myanmar has displaced approximately one million people (OCHA 2018), and the Myanmar government has been accused of ethnic cleansing.

Similarly, in Pakistan the concept of freedom of religion and belief is sensitive and complicated. The minority faith groups in Pakistan not only suffer institutionalised discrimination but also prejudice spread through cyberspace. In April 2018, Pakistan's persecuted Ahmadi minority released an annual report that illustrated how members of the religious sect are consistently targeted by the state. Ahmadis are forbidden from calling themselves Muslims or using Islamic symbols in their religious practices. The report reveals that 77 Ahmadis were booked under discriminatory religious laws in 2017, nine of them remaining in prison, while four Ahmadis were murdered in hate crime across the country. Also, research has shown that Pakistan's media circulated 3 936 news reports and 532 editorial pieces that contained hate propaganda against Ahmadis (Ahmad 2018).

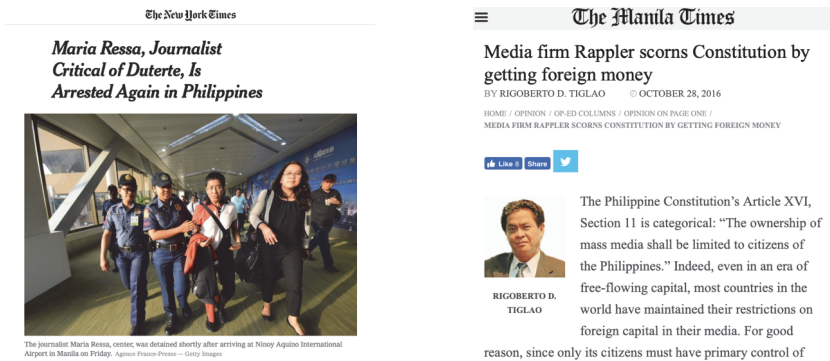
6.3 Digital authoritarianism and human rights in Asia: Freedom of expression and the right to participation

6.3.1 *Troll armies on controlling freedom of expression and shaping public opinion*

Cyber troops of troll armies are the new strategies for governments to control people's expression by shaping public opinion and its opponents. Moreover, the Philippines under the Duterte administration is known as

one of the countries that employ a 'keyboard army' (Palatino 2017; Titcomb 2017; Riley & Pradhan 2018; Coca 2019). There are three methods applied by troll armies under Duterte. First, the troll armies support him during the election process. Many news platforms state that Duterte uses Facebook as a weapon to build support for him and harass his opponents (Stevenson 2019; Riley & Pradhan 2018). Palatino (2017) notes that Duterte's 'keyboard army' consisted of 400 to 500 individuals during the presidential campaign in 2016. The troll army created and distributed messages for the campaign by using both real and fake Facebook accounts. As a result, Duterte dominated the political conversation a month before the vote (Etter 2017).

Second, the drug war that has killed over 20 000 people since 2016 has its policies supported by the troll armies, and criticisms countered. News were shared thousands of times on Facebook by pro-Duterte accounts that claim that Pope Francis blessed the drug war policy at a conference held in the Vatican City (ABS.CBN.com 2018). Since the majority of the population of the Philippines is Catholic, Pope Francis is widely respected. However, the Pope never mentioned the war on drugs.



Source: *The New York Times* 2019 (left) and *The Manila Times* 2016 (right).

Finally, troll armies produce hateful news to support Duterte. One example is the arrest of the journalist Maria Ressa who criticised Duterte's administration (Riley & Pradhan 2018). As of March 2019, Maria Ressa has been arrested three times (Buan 2019). Ressa acknowledged that the attacks on her increased after *Rappler* published how Duterte supporters manipulated Facebook (Stevenson 2019). The government publicly stated that *Rappler* is foreign media that wants to abolish the accountability of its government (*The Manila Times* 2016), and Maria Ressa is a foreign actor.

The Myanmar government also has a keyboard army attached to the military regime, campaigning on Facebook for ethnic cleansing against the country's Rohingya Muslim minority group (Stewart 2019). Since roughly 40 per cent of the population uses Facebook, hateful news spread rapidly.

6.3.2 Communications shutdowns

Shutdowns of communications disrupt human rights advocacy by restricting freedom of expression and participation. In December 2018, the

Bangladesh government blocked Facebook and other social media as well as 4G and 3G mobile data service during its unusual parliament elections (Taye 2019). Moreover, at the same time the government ensured slow internet connections during student protests, and also blocked Skype and shut down several essential news sites (Taye 2019). On 5 August 2018, NetBlock.org tweeted that 'internet disruptions intensif[ied] across #Bangladesh today, particularly in and around #Dhaka. Data suggests targeted, localised just-in-time blocking in response to the protest, threatening #PressFreedom and safety' (NetBlock 2018). Slow connections indirectly reduce people's participation in the democratisation process.

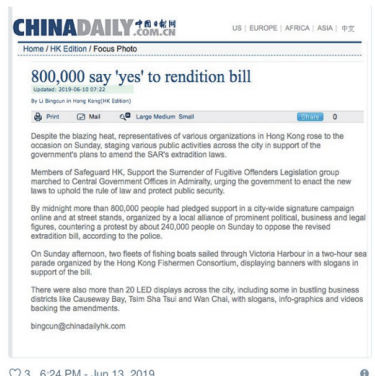
Nevertheless, internet shutdowns also prevent misinformation and hoaxes. In Sri Lanka, the government shut down the internet, including Facebook, Twitter, along with YouTube and Viber, a few hours after bombings on Easter Sunday when 300 people died and many others were injured. The next day, the government extended the shutdown by blocking the website of a VPN service (Vox.com 2019). There is no doubt that the serial bombing created panic, and Facebook could not filter out the false information. Furthermore, families who were looking for their members faced difficulties. However, some people supported this strategy. One senior said that 'what the Sri Lanka government did was authoritarian, but it is also probably what needed to be done to prevent social media from really throwing fuel onto this fire afterward' (Vox.com 2019).

In May 2019, the Indonesian government slowed down the internet and social media network, and restricted the sending of pictures and videos to prevent hoax misinformation as a consequence of a violent demonstration wherein eight people died. Supporters of Prabowo, a presidential candidate who lost the election, staged a demonstration. The National Electoral Commission declared the candidate Jokowi, the winner, leading to protests by opposition groups. There was a dispute over who killed the protestors, resulting in a lack of clarity as to who should be held responsible. To halt tensions, the government shut down the internet (*The Jakarta Post* 2019). This may be interpreted as useful in terms of restricting misinformation or it could be problematic. Furthermore, the government provided neither a report on human rights violations in respect of the demonstration, nor to justify the shutdown (Amnesty International Indonesia 2019).

Blocking and content removal: Government Cyber-Control Centres



Left: One of the headlines of *People's Daily*, a newspaper in Mainland China (inksstonews.com 2019)



Right: Fake news about Hong Kong protest from *China Daily* newspaper (2019)

Another practice is the blocking and removal of content, used by the Chinese government. The picture in *People's Daily* shows a Hong Kong protest in June 2019. This was never a headline on the China mainland where the media blocked the information, while the left picture shows the mainland newspaper's attempt to prejudice the protest. The two pictures above demonstrate how the China government controls information. Ziccardi (2013: 249-250) explains that China is the only country that applies a complex filtering system based on a list of several forbidden keywords, such as democracy, freedom (and all compounds and derivatives, such as Free-China and Free-Net), corruption, children of party leaders, empty chair, and all words related to hatred 'Three T's' (Tibet, Tiananmen and Taiwan) (see also King 2014: 1-10; Perry & Roda 2017: 95-129). The government also has 'The 50 cent party' which produces and manipulates content for blogs and popular media websites, and ensures censorship consistency by trolling the websites in order to find and remove any unacceptable content. They prefer to remove those questionable materials that allow dubious content to circulate freely (Ziccardi 2013: 250).

The authoritarianism in Asian governments seems increasingly to converge. In China, the government established the system decades ago by integrating its system, policy, and troll. Meanwhile, ASEAN countries and Japan started their cyber security not merely as a training programme, but also as the first step towards developing a regional system. In Thailand, the programme could help them control and block information, possibly leading to restrictions on human rights defenders.

7 Arrests, detention, gagging, killings/assassinations

This part explains the restrictions put on human rights defenders in the digital space. The previous parts outline the indirect impact on human rights defenders's rights to participation through content removal and the

misuse of information. This part discusses the direct impact caused by state and non-state actors on the lives of human rights defenders, journalists and media critics, through arrests, detentions, gagging or assassination, looking at examples from countries such as Pakistan, Laos, Vietnam and Cambodia.

Pakistan is the fourth most dangerous country in the world for journalists, with 115 having been killed since 1990, as of May 2019. (Baloch & Qammar nd). Pakistan's extremely limited digital space has led many activists and journalists to be kept in detention, arrested and even assassinated. In January 2017, the Office of High Commissioner for Human Rights (OHCHR) reported that four social media and human rights activists (Waqas Goraya, Asim Saeed, Salman Haider and Ahmed Raza Naseer) had been accused of blasphemy, a criminal offence in Pakistan (Kaye 2017). These social media activists were arrested because they were critical of the state of Pakistan.



Salman Haider delivering his poem 'Kafir', Source: YouTube

Salman Haider, a social media activist, poet and lecturer, was abducted on 6 January 2017 (Zaman 2017). Along with the other activists, he was accused of spreading blasphemous content on social media because of his poem 'Kafir', a controversial term in Islam, which in Urdu literally means 'someone who knows the truth but rejects it' (Qudosi 2017). Conservative groups in Pakistan challenged his criticism of Islam and the military rule. Haider was released after almost three weeks. However, the whereabouts of the other men arrested with him are unknown (BBC 2017). These arrests demonstrate Pakistan's use of digital authoritarianism on its citizens to censor contents relating to issues concerning Pakistan's state affairs, religion and civil-military relationships.

Following the disappearance of these activists and other cases of blasphemous content on online media, the Pakistan Telecommunications Authority (PTA), which is the main communication channel in Pakistan, started sending out warnings to its mobile subscribers. The PTA sent out texts to millions of users which read 'Uploading and sharing of blasphemous content on internet is a punishable offence under the law. Such content should be reported ... for legal action' (Human Rights Watch

2018). The PTA also exacerbates restraints on political participation by launching media campaigns about penalties for individuals who dare express any political or religious opinions (Digital Rights Foundation 2018). This relates to freedom of expression in the digital space where individuals are not able to freely express their views and opinions on matters the state believes are criminal offences, such as blasphemy.

Activists and critics have also been arrested and detained in Laos, a one-party state that exercises absolute control over media and ranks quite low (171) in the 2019 World Press Freedom Index (Reporters Without Borders 2019). In June 2016, three Laotians were arrested for criticising the Communist State on their social media accounts through anti-Facebook comments and posts (Jha 2016). The 2014 decree on internet freedom mentions that anyone who negatively comments against the government can be arrested or jailed. In Cambodia, a young social media user, Heng Leakhena, was arrested in July 2017 for sharing a video on her Facebook account. The video suggested that the Prime Minister, Hun Sen, and his family had been involved in the killing of a prominent political analyst and scholar, Kem Ley, the previous year (Radio Free Asia 2017). Kem Ley often discussed the extent of the wealth of the family of Hun Sen, who had ruled Cambodia for more than 32 years, in Radio Free Asia (RFA) Khmer Service (RFA 2017). Heng faced arrest for speaking out against the government and criticising the Cambodian People's Party (CPP).

Vietnam is another example where digital authoritarianism practices are prevalent. According to the database of The88project.org (2019), a non-governmental organisation (NGO) that supports and encourages freedom of expression in Vietnam, reported that since 2003 at least 13 activists have been arrested. Most of these activists were the supporters of democratisation in Vietnam. One arrested activist, Nguyen Dinh Khue, often posted articles on current national issues and criticised the government on Facebook. He was arrested on 30 April 2019 during the crackdown on the occasion of Vietnam's Reunification Day along with two other activists who also actively posted on the same issues on their Facebook accounts (The88project.org 2019). Nguyen and other activists in Vietnam, who have actively spoken out against Vietnam's government through social media, were arrested and detained (The88project.org 2019).

8 Conclusion

Many Asian governments have used information and communication technologies to invade privacy, deny access to information and spread misinformation, and limit expression and political participation. States that are democratic or repressive are practising digital authoritarianism. Troll armies are used, as in the case of in the Philippines under Duterte, to create content supporting the government and to lambast critics, while communication shutdowns in Bangladesh, are more common. Internet shutdowns in Sri Lanka and in Indonesia to prevent misinformation regarding the election impacted adversely on human rights advocacy. Content blocking and removal act as barriers to human rights defenders. India and Thailand have cases of fake news and misinformation. Myanmar and Pakistan rank high in terms of the proliferation of hate speech, racism and discrimination. Critics, including human rights activists and

journalists, face arrest, detention, or even extra-judicial killings for their opinions in countries hit by terrorism, such as Pakistan.

When George Orwell wrote *1984*, few people imagined that the events he described – horrifying, threatening, distasteful – would ever materialise. Today, 70 years later, the situation has changed radically. New technologies, in the hands of well-meaning people, are useful tools in advancing human rights. In the wrong hands, however, those rights may be threatened using the very same technologies. The dystopian society Orwell imagined is here and now. The world must ensure that this is not also our future.

References

- Agences France-Presse ‘Fact check: No, Pope Francis did not bless Duterte’s administration’ ABS.CBN News, 13 December 2018 [online], available at <https://news.abs-cbn.com/news/12/13/18/fact-check-no-pope-francis-did-not-bless-dutertes-administration> (last visited 27 June 2019)
- Ahmad I Pakistan’s ‘Ahmadi community faces persecution, hate crime: Report’ *Hindustan Times* 28 April 2018, available at <https://www.hindustantimes.com/world-news/pakistan-s-ahmadi-community-faces-persecution-hate-crime-report/story-AuTwmNKaYA63pQwHqrX7oK.html> (last visited 24 April 2019)
- Amnesty International Indonesia ‘Penjelasan polri terkait kekerasan 21-23 Mei 2019 mengecewakan keluarga korban tewas’ (Explanation from national police is disappointing the families’ victims of protest on 21-23 May), <https://www.amnestyindonesia.org/penjelasan-polri-terkait-kekerasan-21-23-mei-mengecewakan-keluarga-korban-tewas> (last visited 27 June 2019)
- Ang YY ‘Autocracy with Chinese characteristics’ *Foreign Affairs* May/June 2018, available at <https://www.foreignaffairs.com/articles/asia/2018-04-16/autocracy-chinese-characteristics> (last visited 15 June 2019)
- Anwar R ‘Challenges of hate crimes in Pakistan’ *Intersections Blog* 14 July 2014, available at <http://www.intersections.org/challenges-hate-crimes-pakistan> (last visited 24 April 2019)
- Baloch H & Qammar ‘A danger of digital surveillance. Bytes for all publications’ (nd), available at <https://content.bytesforall.pk/publication/dangers-digital-surveillance>> (last visited 10 February 2019)
- Bangkok Post ‘Future Forward leaders fight computer crime charge’ *Bangkok Post Online* 17 September 2018, available at <https://www.bangkokpost.com/thailand/politics/1541550/future-forward-leaders-fight-computer-crime-charge> (last visited 27 June 2019)
- BBC News ‘China: The world’s biggest camera surveillance network’ BBC News 2017 (video online), available at <https://www.youtube.com/watch?v=pNf4-d6fDoY&t=140s> (last visited 27 June 2019)
- Bingcun L ‘800,000 say “yes” to rendition Bill’ *ChinaDaily.com* 10 June 2019, available at http://www.chinadaily.com.cn/hkedition/2019-06/10/content_37478727.htm (last visited 27 June 2019)
- Breuer A ‘The role of social media in mobilising political protest: Evidence from the Tunisian revolution’ 2012 Bonn: German Development Institute, available at

- https://www.die-gdi.de/uploads/media/DP_10.2012.pdf (last visited 14 June 2019)
- Brown N 'Liar, liar, platforms on fire: The rise of misinformation and what to do about it' *The SpinOff*. InternetNZ, 4 February 2019, available at <https://the-spinoff.co.nz/partner/internetnz/04-02-2019/liar-liar-platforms-on-fire-the-rise-of-misinformation-and-what-to-do-about-it/> (last visited 23 April 2019)
- Buan L 'Maria Ressa arrested at NAIA over anti-dummy law' *Rappler.com* 29 March 2019, available at <https://www.rappler.com/nation/226880-maria-ressa-arrested-naia-anti-dummy-law-case-march-29-2019> (last visited 23 April 2019)
- Clark J et al 'An uptake in communications encryption is tempered by increasing pressure on major platform providers; governments expand content restriction tactics' *The Shifting Landscape of Global Internet Censorship*. *Internet Monitor* 29 June 2017, available at <https://thenetmonitor.org/research/2017-global-internet-censorship> (last visited 23 April 2019)
- Coca N 'The rise of disinformation and censorship in South-East Asia' *Equaltimes.org* 1 February 2019, available at <https://www.equaltimes.org/the-rise-of-disinformation-and#.XL7rjqeB3MI> (last visited 23 April 2019)
- Digital Rights Foundation 'Content regulation in Pakistan's digital spaces' June 2018 Human Rights Council Report, Digital Rights Foundation, available at <https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/DigitalRightsFoundationSubmissionSpecialRapporteurFreedomofExpression.pdf> (last visited 10 February 2019)
- DW.com 'Indonesia blocking social media to "maintain democracy"' DW.Com 25 May 2019, available at <https://www.dw.com/en/indonesia-blocking-social-media-to-maintain-democracy/a-48858283> (last visited 27 June 2019)
- Etter L 'What happens when the government uses Facebook as a weapon?' *Bloomberg.com* 7 December 2017, available at <https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook> (last visited 23 April 2019)
- Fernandez B 'Fake news in Asian politics' *Global Risk Insights* 1 April 2019, available at <https://globalriskinsights.com/2019/04/fake-news-in-asian-politics/> (last visited 24 April 2019)
- Freedom House 'The rise of digital authoritarianism' Freedom House 2018, available at https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf (last visited 25 February 2019)
- Glasius M 'What authoritarianism is ... and is not: A practice perspective' (2018) 94 *International Affairs* 515, available at <https://academic.oup.com/ia/article/94/3/515/4992409> (last visited 10 March 2019)
- Glasius M & Michaelsen M 'Illiberal and authoritarian practices in the digital sphere' (2018) 12 *International Journal of Communication* 3795
- Halpin EF & Hick S 'Information: An essential tool for human rights work' in S Hick, EF Halpin & E Hoskins (eds) (2000) *Human rights and the internet* London: Macmillan Press 238
- Hintz A & Milan S 'Through a glass, darkly: Everyday acts of authoritarianism in the liberal West' 2018 12 *International Journal of Communication* 3939
- Human Rights Watch 'Pakistan Events of 2017' 2018, available at <https://www.hrw.org/world-report/2018/country-chapters/pakistan> (last visited 10 February 2019)
- Jain D 'The rising trend of child abductions in India' *Live Mint Online* 11 July 2018, available at <https://www.livemint.com/Politics/Bv4TbeToCpVS9j4IX3hJjN/The-rising-trend-of-child-abductions-in-India.htm> (last visited 27 June 2019)

- Jha P 'Laos cracks down on social media critics' *Al Jazeera* 6 June 2016, available at <https://www.aljazeera.com/news/2016/06/laos-cracks-social-media-critics-160606092251543.html> (last visited 17 April 2019)
- Kaye D 'UN expert urges Pakistan to locate and return home four disappeared rights and social media activists' OHCHR News 11 January 2017, available at <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21074> (last visited 9 February 2019)
- King G, Pan J & Roberts ME 'Reverse-engineering censorship in China: Randomised experimentation and participant observation' (2014) 345 *Science* 1
- Linz JJ (2000) *Totalitarianism and authoritarianism* Boulder: Lynne Rienner Publishers Inc
- Lucas L & Feng E 'Inside China's surveillance state' *Financial Times* 20 July 2018, available at <https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543> (last visited 29 March 2019)
- Ma A 'China has started ranking citizens with a creepy "social credit" system: Here's what you can do wrong, and the embarrassing, demeaning ways they can punish you' *Business Insider* 29 October 2018, available at <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4> (last visited 27 June 2019)
- Marr B 'Chinese social credit score: Utopian big data bliss or black mirror on steroids?' *Forbes Online* 21 January 2019, available at <https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#741c3a2a48b8> (last visited 27 June 2019)
- Matsuzawa M 'Duterte camp spent \$200 000 for troll army, Oxford study finds' *Philstar.com* 24 July 2017, available at <https://www.philstar.com/headlines/2017/07/24/1721044/duterte-camp-spent-200000-troll-army-oxford-study-finds> (last visited 27 June 2019)
- Mayer J 'How Russia helped swing the election for Trump' *The New Yorker* 24 September 2018, available at <https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump> (last visited 15 June 2019)
- Mayer S 'China steps up internet surveillance by recording user activities' *CPO Magazine Online News* 19 December 2018, available at <https://www.cpomagazine.com/data-privacy/china-steps-up-internet-surveillance-by-recording-user-activities/> (last visited 23 April 2019)
- Masuda Y (1980) *The information society as post-industrial society* Tokyo: Institute for the Information Society
- Mérieau E 'Thailand's deepening authoritarian rule' *East Asia Forum* 30 January 2018, available at <https://www.eastasiaforum.org/2018/01/30/thailands-deepening-authoritarian-rule/> (last visited 17 June 2019)
- Michaelsen M & Glasius M 'Authoritarian practices in the digital age' (2018) 12 *International Journal of Communication* 3788
- Murakami Wood D 'Editorial: The global turn to authoritarianism and after' (2017) 15 *Surveillance and Society* 357
- Netblocks 'Mobile internet speeds restricted in Bangladesh amid student protest' *Netblocks.org* 4 August 2018, available at <https://netblocks.org/reports/bangladesh-internet-shutdown-student-protests-jDA37KAW> (last visited 23 April 2019)
- Nilsen AG 'An authoritarian India is beginning to emerge' *The Wire* 31 August 2018, available at <https://thewire.in/politics/an-authoritarian-india-is-beginning-to-emerge> (last visited 19 June 2019)

- Office for the Coordination of Humanitarian Affairs *Rohingya refugee crisis* United Nations Office for the Coordination of Humanitarian Affairs 29 August 2018, available at <https://www.unocha.org/rohingya-refugee-crisis> (last visited 27 June 2019)
- Open Net Initiative 'After the Green Movement: Internet controls in Iran, 2009-2012' 2013 Open Net Initiative, available at <https://opennet.net/sites/opennet.net/files/iranreport.pdf> (last visited 15 March 2019)
- Palatino R 'Beware Duterte's troll army in the Philippines' *The Diplomat*.com 18 November 2017, available at <https://thediplomat.com/2017/11/beware-dutertes-troll-army-in-the-philippines/> (last visited 23 April 2019)
- Perry S & Roda C (2017) *Human rights and digital technology: Digital tightrope* London: Palgrave Macmillan
- Qudosi S "'Kafir" poem by Salman Haider' 2017, available at <http://muslimreformers.com/2017/03/21/kafir-poem-by-salman-haider-translated/> (last visited 10 May 2019)
- Radio Free Asia 'Young Cambodian arrested for derogatory comments about Hun Sen on social media' Radio Free Asia 13 July 2017, available at <https://www.refworld.org/topic,50ffbce582,50ffbce58e,5a0f01d64,0,,KHM.html> (last visited 28 June 2019)
- Reporters Without Borders 'Laos: No light under the tunnel' Reporters Without Borders for Freedom of Information 2019, available at <https://rsf.org/en/laos> (last visited 10 February 2019)
- Riley M & Pradhan B 'A global guide to state-sponsored trolling' *Bloomberg*.com 19 July 2018, available at <https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/> (last visited 23 April 2019)
- Ruijgrok K 'From the web to the streets: Internet and protests under authoritarian regimes' (2016) 24 *Democratization* 498
- Santos VO 'The Philippines just became more authoritarian, thanks to the people' *The New York Times* 24 May 2018, available at <https://www.nytimes.com/2019/05/24/opinion/philippines-duterte-election-senate.html> (last visited 18 June 2019)
- Seiff A 'Hate crime, racism on the rise in Southeast Asia' *UCA News*.com 3 July 2014, available at <https://www.ucanews.com/news/hate-crime-racism-on-the-rise-in-southeast-asia/71321> (last visited 24 April 2019)
- Smidi A & Shahin S 'Social media and social mobilization in the Middle East: A survey of research on the Arab Spring' (2017) 73 *India Quarterly* 196
- Stevenson A 'Maria Ressa, journalist critical of Duterte, is arrested again in Philippines' *The New York Times* 28 March 2019, available at <https://www.nytimes.com/2019/03/28/business/media/maria-ressa-arrested-philippines-rappler.html> (last visited 23 April 2019)
- Stewart E 'Can Facebook be trusted to combat misinformation? Sri Lanka's shutdown suggests no' *Vox.co*, 23 April 2019, available at <https://www.vox.com/2019/4/23/18511640/facebook-sri-lanka-bombing-social-media-attack> (last visited 27 June 2019)
- Sullivan B 'Thailand to host ASEAN-Japan cybersecurity centre to be launched in June 2018' *Thailand Business News* 2 April 2018, available at <https://www.thailand-business-news.com/asean/68592-thailand-to-host-asean-japan-cybersecurity-centre-to-be-launched-in-june-2018.html> (last visited 27 June 2018)
- Tan C 'Malaysian police adopt Chinese AI surveillance technology' *Nikkei Asian Review* 18 April 2018, available at <https://asia.nikkei.com/Business/Companies/>

- Chinas-startup-supplies-AI-backed-wearable-cameras-to-Malaysian-police (last visited 27 June 2019)
- Taye B 'Sudan, Bangladesh, DRC, Gabon start 2019 with major digital rights violations' Accesnow.org 10 January 2019, available at <https://www.accessnow.org/sudan-bangladesh-drc-gabon-start-2019-with-major-digital-rights-violations/> (last visited 23 April 2019)
- Tehusijarana KM & Valentina J 'Jakarta riot: Government temporarily limit access to social media, messaging apps' *The Jakarta Post* 22 May 2019, available at <https://www.thejakartapost.com/life/2019/05/22/jakarta-riot-government-temporarily-limits-access-to-social-media-messaging-apps.html> (last visited 27 June 2019)
- The 88 Project 'Database of persecuted activist in Vietnam' 2009, available at <https://the88project.org/database/> (last visited 28 June 2019)
- The 88 Project 'Nguyen Dinh Khue' 2018, available at <https://the88project.org/profile/373/nguyen-dinh-khue/> (last visited 28 June 2019)
- Tiglao RD 'Media firm Rappler scorns constitution by getting foreign money' *The Manila Times* 28 October 2016, available at <https://www.manilatimes.net/media-firm-rappler-scorns-constitution-getting-foreign-money/293543/> (last visited 27 June 2019)
- Titcomb J 'Governments in 30 countries are paying "keyboard armies" to spread propaganda, report says' *Telegraph* 14 November 2017, available at <https://www.telegraph.co.uk/technology/2017/11/14/governments-30-countries-pay-keyboard-armies-spread-propaganda/> (last visited 23 April 2019)
- Tortermvasana K 'Cybersecurity ASEAN course set for June' *Bangkok Post* 30 March 2018, available at <https://www.bangkokpost.com/world/1437530/cybersecurity-asean-course-set-for-june> (last visited 27 June 2019)
- Xueying N 'Many people refused to accept military service into the blacklist of credit information' *Beijing News* 19 March 2018, available at <http://www.bjnews.com.cn/news/2018/03/19/479533.html> (last visited 27 June 2019)
- United Nations *Report of the independent international fact-finding mission on Myanmar* United Nations Human Rights Council (2018)
- Wagner B 'Understanding internet shutdowns: A case study of Pakistan' (2018) 12 *International Journal of Communication* 3917
- Zaman A 'Digital activists are disappearing in Pakistan' *Global Voices* 2017, available at <https://advox.globalvoices.org/2017/01/12/digital-activists-are-disappearing-in-pakistan/> (last visited 27 June 2019)
- Zhou V 'Mainland Chinese evade censors to support Hong Kong protest' *Inkstonenews.com* 13 June 2019, available at <https://www.inkstonenews.com/politics/chinese-internet-users-evade-censors-support-hong-kong-protests/article/3014352> (last visited 27 June 2019)
- Ziccardi G (2013) *Resistance, liberation technology and human rights in the digital age* Netherlands: Springer

Sustaining human rights in the era of new technologies: Case studies of Armenia, Belarus and the Kyrgyz Republic

Aisuluu Abdubachaeva,* *Kristina Vavrik*,**
Karen Ayvazyan,*** *Mariam Mkrtchyan***** and
*Yuriy Nosik******

Abstract: *The development of new technologies and innovation is meant to enhance accessibility and make life easier. Due to the fast pace of development, the response of countries to new technologies is crucial to ensure their reasonable use. However, along with the development of new technologies different implications have emerged as some developing countries appear not to be capable of effectively responding to these developments. Despite the positive impact of new technologies on various aspects of life, their misuse has negative implications for the enjoyment of human rights. This article aims to explore regional challenges to human rights caused by new technologies at the national and regional levels. It also aims to identify long-term structural challenges to human rights in Armenia, Belarus and the Kyrgyz Republic with a focus on cyber security, freedom of expression, freedom of speech, access to information and data protection policies. It further aims to make recommendations to stakeholders so as to improve the situation and minimise the negative impact of new technologies on human rights. On the one hand, the study reveals that the development of new technologies increased the accessibility of people to information in terms of e-governance programmes. Moreover, it shows that political mobilisation and participation, and freedom of expression have been enhanced due to social media developments. On the other hand, it identifies the current challenges to human rights in Armenia, Belarus, and the Kyrgyz Republic in terms of increasing hate speech online, media manipulation, the spreading of disinformation, data leakage and cyber security. The study shows that despite the positive impact of the new technologies on the enjoyment of human rights, the inability of these states to effectively respond to the developments and eliminate the misuse of new technologies, and the insufficiency of strategies, legislation and policies, are negatively impacting on human rights.*

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. MA in Human Rights and Democratisation, Centre for European Studies, Yerevan State University; aisuluu.abdubachaeva87@gmail.com

** MA in Human Rights and Democratisation, Centre for European Studies, Yerevan State University; k.vavryk@gmail.com

*** MA in Human Rights and Democratisation, Center for European Studies, Yerevan State University; ayvazyan.karen@gmail.com

**** MA in Human Rights and Democratisation, Center for European Studies, Yerevan State University; mkrtchyanm27@gmail.com

***** PhD (Law); Associate professor of law, Taras Shevchenko National University of Kyiv; yuriy.nosik@gmail.com

Key words: *human rights; digitalisation; cyber security; new technologies; e-governance; freedom of speech; free flow of information; digital rights*

1 Introduction

Scientific and technical progress has led to the emergence of new information and communication technologies (ICT), which have both a positive and a negative impact on individuals' lives and on society. On the one hand, ICT have simplified access to information and significantly improved the communication landscape. People have become able to freely overcome geographic, political, and social barriers in order to build social interaction in a fairly short period of time. Moreover, the progress of ICT enhanced the concepts of e-democracy and the role of media as a facilitator of political mobilisation. In addition, the development of new technologies has contributed to the increased transparency and openness of the activities of the authorities. Of equal importance is the fact that the development of ICT has influenced the implementation and protection of a number of fundamental human rights. However, at the same time it became evident that these new technologies have become tools of manipulation, the spreading of disinformation, hate speech and data interception.

The use of social media networks, especially Facebook, Twitter, Telegram and Instagram has significantly increased over the past ten years. In this sense, online space is being actively used by different civil society organisations (CSOs) to reach a wider audience. For example, Facebook groups or pages are being created to serve as an effective tool for communication with the public to ensure timely responses in decisive situations. In addition, enhanced coverage of events by both local and international media (especially intensive live streaming) has constrained the radical actions of the government in relation to the public. However, the enhanced use of new technologies may lead to several human rights violations. What is at issue is the dissemination of hate speech, the use of individuals' personal data for unjustified purposes, and so forth. In addition, a strong relation between the rapid integration of information technology and cyber security was found, which raises questions about a number of security problems and their solutions, ranging from technical to legislative. The cyber security problem is one of the most pressing issues in the region, especially given its historical-political context. The latter refers to territorial conflicts and the geopolitical interest of major superpowers in the region.

Despite the relevance and importance of this topic, there is no comprehensive research in the field that addresses the challenges of new technologies to human rights in the region. The present research for the first time explores the impact of new technologies on the enjoyment of human rights in Armenia, Belarus and the Kyrgyz Republic. It explores possible mechanisms to prevent the violation of human rights with regard to the new technological developments.

The article aims to explore regional challenges to human rights caused by new technologies. It also aims to identify long-term structural challenges to human rights in Armenia, Belarus and the Kyrgyz Republic with a focus on cyber security, freedom of expression, freedom of speech, access to information and data protection policies, and to make

recommendations to the stakeholders to improve the situation and minimise the negative impact of new technologies on human rights.

The methodological approach adopted in the study is a mixed methodology based on the comparative and contrast analysis of the previous research on the topic, case studies and legal analysis of current legislation and regulations of Armenia, Belarus and the Kyrgyz Republic.

The main body of the report consists of three parts. Part 2 presents the Armenian case study of the topic; part 3 introduces the overall impact of new technologies on freedom of expression and freedom of speech in Belarus; and part 4 provides detailed information on the impact of new technologies on human rights in the Kyrgyz Republic.

2 Positive and negative impact of new technologies on the enjoyment of human rights: A case study of Armenia

This chapter presents how the rapid integration of ICT in the era of globalisation has affected the implementation of a number of fundamental human rights in Armenia and proceeds to describe the role of digital activism in providing even greater scope for democratic participation and decision making during the Armenia's Velvet Revolution. At the end of the section, the negative impact of the new technologies on individuals' lives and society is discussed, taking into account the historical-political context of the country.

2.1 The role of social media in political mobilisation: Armenian Velvet Revolution

The advancement of information and communication technologies in the era of globalisation has turned media into one of the most powerful factors in influencing the processes occurring in the world. This specifically refers to the fact that by means of social media it has become possible to promote a number of fundamental human rights, in particular the rights of peaceful assembly (article 21 of the International Covenant on Civil and Political Rights (ICCPR)), association (article 22 of ICCPR), freedom of opinion and expression (article 19 of ICCPR) and so forth. In this regard, social media has become a means of encouragement of a two-way political communication between the public and the authorities.

Digital activism or cyber-activism is a good example of how traditional notions of human rights have been complemented by a new phenomenon that provides an even greater scope for democratic participation and decision making. Digital activism, characterised by the substantial use of social networks as the main platforms to set up information campaigns and mobilise the masses, was the key factor of success of the Velvet Revolution in Armenia (2018).

In general, cyber-activism in Armenia touches upon many aspects of life: from controversial social principles to dissatisfaction with government policies. Activists deliberately choose social networks such as Facebook for the promotion of common ideas because of its worldwide targeting and transparency. The latter coincides with the principles for which these persons of influence are engaged in the political struggle. At the same time, Facebook is attracting the attention of political and economic elites as

many of them are active users thereof. By using Facebook, activists appeal to their multi-million diaspora. Members of the diaspora, especially those in the United States and Russia, are prominently participating in the political and financial life of Armenia. For this reason, the bulk of user-generated content is written in Armenian, English and Russian.

Over the past 10 years, numerous mass protests were staged in Armenia to express dissatisfaction with the government policies. However, the entire population did not seek to mobilise, but left the steering wheel in the hands of the youth. The case of the Velvet Revolution was somewhat different. When the protest action Take A Step was launched by the leader of the opposition, Nikol Pashinyan, both the youth and adults contributed to the common goal. The reason why in this case the majority of the population sought to take part in the country's political life was conditioned by the impact of digital activism that was causing a snowball effect.

Since the oppositionists mostly appealed to the youth, the first snowball was transmitted to them, thereby inspiring the latter to actively engage in the promotion of an online campaign on Facebook, called *Dasadul* (or 'class strike').¹ The campaign was aimed at encouraging students to skip lessons in order to participate in anti-government protests. On Facebook, special events were created almost daily to provide the interested citizens with all the necessary information as to when and where they needed to gather to start the march.

Another social network actively used during the Velvet Revolution to promote the idea of customer boycott was Telegram. By means of a special channel named Baghramyan 26, information was disseminated among its subscribers as to which supermarkets they needed to avoid using since the latter were the property of political and economic elites (for instance, Yerevan City and SAS supermarkets). The same information was shared by different groups on Facebook, mainly run by the youth.

Another form of the manifestation of discontent was the creation of a number of digital products that reflected the peaceful nature of the revolution, namely, songs (for instance 'Dukhov' ('Risk bravely'), 'Nikol Pashinyan'),² short documentary films, and so forth. These were necessary not only to convey key messages to authorities in a peaceful manner but also in order to gain the attention of third parties (that is, of the international community) towards domestic affairs.

The adult population did not yield to the youth. In their turn, professionals in the field of education were running online petition campaigns on their social networks, which were directed at supporting youth activists who had been arrested as a result of their participation in the protests, as this would undermine the value of a number of

1 These were the founders of the 'Restart Student Initiative', key drivers of the Velvet Revolution in Armenia, who coordinated the whole process and created on Facebook special events for the promotion of *Dasadul*, available at <https://www.facebook.com/events/369494443572566/> (last visited 10 March 2019).

2 It is interesting to note that the word *dukhov* – a slogan that was very popular in social media and which was depicted on the hats and T-shirts of the protesters – became a real trend even after the revolution had ended.

fundamental human rights, including the right of peaceful assembly, association, and so forth.

Hence, the case of the Velvet Revolution serves as a good example of how new information technologies can help to exercise a number of fundamental civil and political rights and to create various digital products, capable of awakening people's politicised identity and mobilising them.

2.2 Open digital space: Fertile ground for hate speech, manipulation and the spreading of disinformation

With the development of new technologies the accessibility to information has also increased during recent years and the use of social media facilitates the spreading of this information. However; in countries where media literacy is not highly developed and where most social media users lack certain competences to differentiate real news from fake news, they easily obtain 'trapped' disinformation. As is mentioned in the Media Sustainability Index 2018 report, online media provides more varied viewpoints than the television outlets, but another problem arises here, namely, that '[t]he news feed, and the flow of fake news is so abundant that a public with quite low media literacy levels becomes ripe for manipulation' (IREX 2018: 5). Social media manipulations have escalated in Armenia, especially over the past year, when the opposition tried to bring up false agendas to discredit the previous government, which managed to win the sympathy of the vast majority in the country. Thus, the problem of media literacy, which arises with the development of new technologies and the manipulative use of social media, on the one hand, and a lack of literacy, on the other, has a negative impact on the wider public. Additionally, the manipulation leads to the hate speech towards certain groups, politicians or the government itself.

Another trend that has been very popular in Armenia, especially before the parliamentary elections in 2018, is online campaigning through fake accounts. Certain politicians or political parties make use of new technologies and social media and freedom of social media in Armenia to create fake accounts in order to manipulate the public with their false agendas. The fake accounts usually spread false information on behalf of the Prime Minister or the leading party in order to create mistrust towards the government and discredit the Prime Minister as well as to create an impression of enjoying popularity among the public. According to the investigations of the Union of Informed Citizens, a non-profit organisation, one of the major political parties (Prosperous Armenia) used 390 fake accounts on social media during its election campaign to create an impression of having a high level of support online (Fact Investigation Platform 2018).

In the post-election period more fake pages on Facebook were created on behalf of the Prime Minister and with the slogans of Velvet Revolution in order to attract more attention and get more followers who would be the target of the manipulation and disinformation. Based on the reactions of the public, who mostly believed in the disinformation provided to them as well as hate speech online and online extremisms, the Prime Minister had to ask the national security service to investigate and trace the people behind these fake accounts. Following the order, one of the fake account

users was arrested for spreading racial and ethnic hatred and discrimination online.

The extensive use of social media for political purposes could often entail negative consequences such as the spread of hate speech. In Armenia, by virtue of its strong conservative values, the representatives of the lesbian, gay, bisexual and transgender (LGBT) community often become the targets of hate speech. The social media is being ‘served’ for people to express their opinions about different topics and mostly the reaction of the public to the posts about LGBT activities and opposition thereto. A content review of the posts on social media about the above-mentioned targets by the most popular online newspaper shows that 82 per cent of the comments observed contained hate speech towards the LGBT community and a transgender woman who has spoken at the National Assembly, whereas 18 per cent were either neutral or combating comments without hatred. Moreover, another post on the LGBT community received 67 per cent hatred comments, and 33 per cent of combating or neutral comments without hate speech. In another case, a post about a member of the opposition, Armen Ashotyan, received hatred comments from 75 per cent of the commentators, while 25 per cent expressed neutral views on the topic and the politician itself (Table 1). Thus, the content analysis reveals that the social media is used to spread hatred towards the vulnerable groups and the opposition.

Table 1: Hate speech in the comments on social media

Facebook post content	Total number of comments	Sample	Percentage comments containing hate speech	Percentage of neutral comments
A transgender woman has spoken at the National Assembly https://bit.ly/2ULKmOb (Azatutyun TV)	1944	First 50 comments	82% (41)	18% (9)
An opposition leader, Armen Ashotyan, about the 2nd President, Robert Kocharyan, being a political prisoner https://bit.ly/2XBE9Bn (Aravot Online Newspaper)	216	First 20 comments	75% (15)	25% (5)
Article about LGBT community becoming more active in Armenia after the Velvet Revolution (Blognews.am) https://bit.ly/2Ve2xeV	97	First 15 comments	67% (10)	33% (5)

It is worth noting that, in general, the regulations of hate speech in Armenia are rather limited. Article 226 of the RA Criminal Code (2003) covers only national, racial or religious hatred. The first part of the article claims that ‘actions aimed at incitement of national, racial or religious

hatred, at racial superiority of humiliation of national dignity are punished' (chapter 26). However, no protection is guaranteed against incidents 'on the grounds of sexual orientation or gender identity'.

It is interesting to note that in practice, article 226 of the Armenian Criminal Code has hardly ever been applied, thereby provoking an atmosphere of impunity. During the Velvet Revolution most of the members of the national conservative party (Republic Party of Armenia) became the targets of hate speech. The latter was the ruling party of Armenia for 20 years and was often associated as a 'post-Soviet ruling party with catch-all ideology'.

When opposition leaders started their protest action Take A Step, the rhetoric of most of them was inflammatory. They were constantly emphasising the division of society into 'us' (that is, the supporters of the revolution) and 'them' (that is, those who were on the side of the Republican Party), giving rise to more incidents of hate speech and offending posts accompanied by memes.

2.3 Rapid integration of information technology in governance: Cyber security in Armenia

Considering the above-mentioned, it becomes clear that everyday society is becoming more dependent on information and communication technologies. Even more crucial is the protection of these technologies for the sake of the national interest.

The development of new technologies makes people's lives easier especially when it comes to accessing or requesting information online. However, it also presents some vulnerability in terms of cyber security. The Armenian government adopted e-governance several years ago, which gives people easier access to information. However, open access to certain information leads to the violation of human rights in terms of data protection. The latest example is Armenia's online voters' register elections.am, the aim of which is to provide citizens with information on locations of district electoral commissions (DECs). The website is developed in such a way that once a citizen (voter) enters some personally identifiable information in special columns, the voter finds information according to the residential address. At first glance this seems to be a good thing, but the problem is that any citizen of the Republic of Armenia who has the minimum information about another citizen – such as a name, surname and/or date of birth – can find the same information on his/her residential address, the DEC as well as information on that person's family members who are registered at the same address. The former in turn questions the right to privacy of this person and his/her family members (article 17 of ICCPR).

Chapter 2, article 4.2 of the Law of the Republic of Armenia on Protection of Personal Data (2015) states that '[p]ersonal data shall be processed for legitimate and specified purposes and may not be used for other purposes without the data subject's consent' (Law of the Republic of Armenia on Protection of Personal Data 2015). However, in case of elections.am, there is a problem as to whether it was justifiable to make personal information of citizens available to the public since this may also serve as a threat to a person's safety and security. In particular, if the purpose of the website is to provide information on district electoral

commissions, then the former can be developed in such a way as to replace columns with the entry of personal information (name, surname, date of birth, and so forth) with the column where the citizens will need to enter special personal codes, available only to them. The latter is of a huge importance since transparency in this case may serve no good but rather will encroach upon citizens' safety and will also serve as a threat to national cyber security as third parties can also access the information.

The development of the information society raises the issue of cyber security, which raises questions about a number of security problems and their solutions, ranging from technical to legislative.

The International Telecommunication Union (ITU) has published the annual Global Cyber Security Index (GCI) study (2017), which assesses the level of cyber security of states according to five main indicators: legal, technical (including child online protection), organisational, capacity building and cooperation. The study was conducted in 2017 in relation to 193 countries around the world. According to Table 2 it is evident that in the CIS region only Georgia and Russia had high GCI scores, and this was conditioned by their good performance in regard to all five indicators. In contrast, the performance of Armenia was unsatisfactory in all spheres except cooperation. This is the reason why Armenia only took the one hundred and eleventh place in the GCI, while neighbouring Georgia was in the eighth and Azerbaijan in the forty-eighth place (International 2017: 54).

Table 2: Global Cyber Security Index (GCI) 2017. CIS region scorecard³

	Legal measures	Technical measures	Organisational measures	Capacity Building	Cooperation	GCI Score
Armenia	Low	Low	Low	Low	Medium	Low (0,196)
Azerbaijan	Medium	High	Low	Medium	High	Medium (0,559)
Belarus	High	High	Medium	High	Medium	Medium (0,592)
Georgia	High	High	High	High	High	High (0,819)
Kazakhstan	Medium	High	Low	Low	Low	Low (0,352)
Moldova	Low	High	Medium	Low	Medium	Medium (0,418)
Russia	High	High	High	High	High	High (0,788)
Tajikistan	Medium	Low	Medium	Medium	Low	Low (0,292)
Turkmenistan	Medium	Low	Low	Low	Low	Low (0,133)

3 Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

Ukraine	High	Low	Medium	Low	High	Medium (0,501)
Uzbekistan	Medium	Medium	Medium	Low	Low	Low (0,277)

In this study, the ITU also provided information on particular countries' experiences of applying specific solutions in order to advance their cyber security.

For example, with regard to the legal sphere the importance of having cybercrime legislation was highlighted as was the case in Columbia (one of the first countries to enact law targeting cyberspace), as well as Georgia, which established their cybercrime legislation in accordance with the Budapest Convention. Another key factor mentioned was the provision of cyber security training by the government.

Another important sphere was technical (with important dimensions such as the existence of special technical institutions, online protection of children, and so forth). Referring to examples of certain countries, it was shown that the existence of special computer emergency teams (for instance Egypt's G-CERT and Brazil's CERT) is essential to support the information technology sector and to help the latter to cope with cyber security threats. Significant importance was also attached to children's online protection.

Another sphere mentioned was organisational, implying (i) the development of a cyber security strategy (for instance the UK's National Cyber Security Strategy and Russia's adopted National Security Strategy); and (ii) the creation of a special coordinating agency by a government (for instance the Cyber Security Council of Iceland). In addition, special attention was given to specially-designed public awareness campaigns, as was the case in Latvia. A national portal named CERT has been created so that people can be provided with security solutions, for example, anti-viruses, which are free of charge. Moreover, the CERT is organising a bi-annual special campaign during which people can bring their laptops or computers to establish whether they have been infected.

Thus, if the experience of Armenia is evaluated through the prism of the afore-mentioned thought-provoking practices, it would become clear why it took only the one hundred and eleventh place on the list. Armenia has cybercrime legislation which is enacted through the Penal Code and Law on Electronic Communication, and specially-designed computer emergency response team- CERT-AM, but according to the wellness profile created by ITU (2014, 1–3) it lacks (i) an officially-approved cyber security framework necessary for the implementation of cyber security standards (which are internationally recognised); (ii) a national cyber security strategy and accordingly responsible agencies responsible for its implementation; (iii) sector-specific research and development programmes or projects; (iv) educational and/or professional training on cyber security; (v) partnerships that could have contributed to sharing of cyber security assets of either other states or the public sector (it is only the member of a special ITU-IMPACT initiative); and (vi) a special agency that could have provided institutional support on child online protection (even though Armenia has legislation on children's online protection. The latter is enacted through article 263 of the RA Criminal Code.

The aforementioned illustrates most of the major omissions. This should be rectified and a cyber security commitment should be demonstrated, especially given Armenia's historical-political context. What is at issue is the territorial conflict over Nagorno-Karabakh between two former Soviet countries, Armenia and Azerbaijan. This latter was also manifested in the form of an information war, leading to the dissemination of fake news, hate speeches, and even cyber-attacks which occurred in the winter of 2000 (Arminfo 2019). The attacks were from both sides – Azerbaijan hacked 30 Armenian websites and Armenia launched a counter-attack – and the damage was mutual.

Armenian cyber security expert Samvel Martirosyan also claimed that public facilities such as power stations, gas and water supply systems are becoming vulnerable since they can also be hacked. This is of substantial strategic importance especially due to their contribution to military efficiency/capability.

Martirosyan also stressed that in Armenia there is no special agency that can provide institutional support to solve these issues. This is why Armenia needs to create a special national agency – especially for monitoring and awareness-raising purposes – which already exists in neighbouring countries (Martirosyan 2018). Another important issue to be mentioned is that a special control should be established over crucial non-governmental organisation (NGO) structures such as banking (Arminfo 2019), since most of them are in the possession of foreign investors. The latter implies that some problems may arise not only because of a lack of accountability, but also due to the influence of third countries.

Cyber security issues and the lack of media literacy contribute to the data leakage. People with poor media literacy tend to click on all the links that they receive through email, social media, or advertisements on different unreliable web pages. This leads to the hacking of social media accounts and control over personal user information, including bank account details. This tendency recently became relevant for the applications developed for smartphones. For example, an application called GetContact recently became very popular among Armenians and in the region itself. The application identifies telephone numbers by using the user's contact list, and it emerged that the application uncovers the caller's personal data and photo from its database (Kaspersky 2018).

Hence, referring to what was said above, it becomes extremely important for Armenia to provide institutional support for the development of cyberspace protection mechanisms in conformity with international cyber security and digital regulation practices to avoid threats to the state sovereignty and human rights protection.

3 The impact of new technologies on human rights: A case study of Belarus

This part presents peculiarities of the human rights situation in the Republic of Belarus reasoned by the geopolitical position of the state. It proceeds to explain the importance of new technologies and different sides of its impact on the fulfilment of human rights of Belarusian citizens. Finally, this part emphasises the main challenges and ways to overcome them.

3.1 New technologies and freedom of expression

The Republic of Belarus is a country located between the European Union (EU) and Russia. This geopolitical peculiarity explains many events occurring in the country: on the one hand, Belarus is influenced by Russia and, on the other hand, by the EU. Thus, the impact of Russia on Belarus results in substantially identical legislative provisions regarding the fulfilment of human rights, while the influence from the West is characterised by facilitated development of the new technologies in the country.

New technologies play an important role in the life of Belarusian society in both positive and negative ways. The positive impact consists of accelerating civil engagement, facilitating the communication of the state with civil society and human rights organisations, enhancing monitoring instruments.

Indeed, in recent years engagement of civil society in political life of the state has increased significantly: the Belarusian NGOs engaged in human rights protection regularly organise lectures, seminars and training in an effort to explain how people can protect themselves while using the internet and how to make a difference between a trustworthy information and fake news; a non-commercial platform, Petitions.by, raises awareness and involves millions of Belarusians in a dialog and cooperation with the authorities in a common effort to resolve local, regional and state-level problems. The involvement is carried out through writing, promoting and signing petitions to the relevant authorities with regard to persistent problems bothering citizens of particular districts or regions. At the same time, the Belarusian authorities apply new technologies in the process of governing to facilitate communication with the citizens and make an access to state services easier. Thus, Belarus has made it to the eighteenth position in the rating of countries with the best e-government services (Artezio 2000). Moreover, increased monitoring possibilities have a positive impact on the human rights situation in the state. Now it is possible to get reliable information not just from state entities – the National Statistical Committee of the Republic of Belarus, the National Academy of Science of the Republic of Belarus – but also from civil society as well as national and international human rights organisations that have elaborated their own monitoring systems. The abundance of statistical data allows the situation to be followed and excludes the possibility of even a minute change in the human rights fulfilment going unnoticed. Therefore, it is easy for human rights and civil society organisations to attract the attention of the Belarusian authorities as well as of the international community to problems prevailing in the Belarusian society and, consequently, to accelerate their elimination.

However, enhanced possibilities and easier access to statistical data and monitoring are not the only ways in which new technologies change the human rights status for the better. New technologies applied to the different spheres of society have a very positive impact on the state's economy through the creation of new working places, the increase of incomes via improvement of effectiveness and productivity, and the attraction of investments to the country. Economic growth inevitably leads to better living conditions of society and, consequently, a fuller enjoyment of human rights. A good example of such developments might be presented by the Belarusian Hi-Tech Park, which due to a special IT

environment attracts to Belarus numerous investments in line with dozens of foreign companies, start-ups and initiatives coming to register there every year and creating working places for the Belarusian people, and improving their quality of life.

This is evidence of the positive impact of new technologies on human rights fulfilment. However, reports of international organisations often emphasise overly restrictive legislative provisions on freedom of expression, peaceful assembly and association as well as on freedom of the press. They highlight the resilience of the government to the international pressure and its unwillingness to soften the legislative framework in relation to the freedom of expression and freedom of press/media sources (Human Rights Watch 2019).

Freedom House (2018b) has classified Belarus as ‘not free’ in both the Freedom of the Press and Freedom on the Net 2018 indexes. Such a low score is justified by facts of massive detention of journalists while fulfilling their professional duties, in particular, covering important, even though unfavoured by the authorities, civic and political events in the country. Even though a number of the detentions has decreased by two-thirds since 2017, it remains high (Table 3).

Table 3: *Detentions of journalists in Belarus*⁴

Year	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Ranking	20	30	167	60	54	29	19	13	101	31

Moreover, the government has adopted provisions that limit access of independent online media sources to official information and frequently induces them to employ self-censorship. This poses a serious problem for the fulfilment of the free flow of information. State-led media sources’ coverage is insufficient and unbalanced, it mostly presents official versions of the events, which is roughly informative and does not provide any critical analysis. Thus, for example, the events of the 101st anniversary of the Belarusian People’s Republic (BPR), which took place on 25 March 2019, were at least partly covered by the independent national media sources while state-run media barely mentioned the events of the day and did not present data on detentions of people and reasons of their detention – the use of the Belarusian historical flags and symbols. This means that many people, who do not regularly check online media sources but rather follow television news programmes, are unaware of what is happening in Belarus at the moment and, consequently, cannot make their informed position on the actions of government as well as those of citizens participating in civic and political activities in the country.

At the same time, in 2018 the authorities got arbitrary power to block media sources for a period of three months without a court decision for the alleged violation of restrictions on the press/media (Pravo.by 2003). Ever since there has been a degree of concern among the media, as the

4 Source: <https://baj.by/en/analytics/repressions-against-journalists-belarus-2018-chart>.

adoption of the Media Bill puts at risk every independent media source critical of the government. The legislative framework for the media enshrines a complicated procedure of registration and often discriminatory policies with regard to the independent resources. This often implies limited access to press briefings, government officials as well as less ability to distribute printed materials and higher costs for it (Pravo.by 2003). Moreover, journalists employed at the independent media or freelancing for international media are being detained while carrying out their duties during civil and political actions. Journalists and freelancers of international media sources face an acute problem, because the government frequently denies them accreditation and editorial certificates, putting them on the front line and leading to temporary imprisonment together with the confiscation of their equipment (Table 4).

Table 4: Fines to journalists under 22.9(2) of the Code of Administrative Violations⁵

Year	2014	2015	2016	2017	2018	04/2019
Ranking	10	28	10	69	118	14

Turning to the issue of digital freedom and security, the Belarusian government has imposed no permanent restrictions on connectivity or access to social media sources as well as communication applications. Nevertheless, the government has the ability to control the speed of internet connection due to the fact that only two entities are permitted to control connections within and outside the country – Beltelecom and National Centre for Traffic Exchange, both of which are controlled by the state. Therefore, the authorities not only control the speed of internet connection throughout the country but also monitor users' activities.

3.2 Regulation of the flow of information, digital security and freedom of speech

To understand the status of freedom of information, expression and digital security properly it is necessary to analyse how this field is being regulated. First, it should be noted that in the last few years the topics of freedom of expression, information and digital security have become very pressing and the authorities are working hard on the development of a legislative framework to regulate all activities in the sphere. Thus, in 2018 the Media Bill was revised (Pravo.by 2003), and drafted a new law on personal data protection (Forumpravo.by 2013), the adoption whereof is planned for the first half of this year. The national concept of information security was also adopted recently (President.gov.by 2019), that is the most important document providing a basis for the development of relevant legislative provisions and defining directions for the state policy.

In December 2018 the amendments to the Media Bill entered into force, raising concern in the Belarusian media sphere (Belarus.by 2009). The revised law stipulates the following:

5 Source: <https://baj.by/en/content/article-229-code-administrative-violations>.

- the obligation of owners of internet resources – bearing any of the national domains .BY or .BE/L – to identify its subscribers;
- compulsory pre-identification of the users to connect to public WiFi;
- the obligation of online media sources to register and obtain the official status of mass media resource in order to have access to the official information;
- the broadening of the list of prohibited information, which now became even more vague and open for interpretation for the authorities. In this light, it includes propaganda of unhealthy lifestyles, drug use, disrespect for different social, national, ethnic and religious groups, xenophobia, extremism, and so forth.

Moreover, the list of prohibited information is not fully presented in the Concept (President.gov.by 2019) or other legislative provisions. Several types of information are provided, but in the end it is always mentioned 'and other kinds of prohibited information stipulated in legislation of the Republic of Belarus'.

These provisions raised broad concerns in society, and particularly among the Belarusian online media sources, when they were first denounced. For the users such provisions inevitably imply a broader collection of users' personal data. This may be regarded as an infringement upon private life and freedom of expression of Belarusian internet subscribers. However, the state has a different perspective on the issue. By the identification and collection of users' data the state seeks to prevent cybercrimes and attacks and, thus, to protect society from prospective risks. It has been said that the state aims at ensuring the safety of collection, processing and storage of the users' data in order to protect their rights.

Turning to the provision on registration of online media, this was met by an even broader public discussion, because basically such provision enshrined the inequality of rights and access between state-led and independent online media sources, which even before faced numerous obstructions while doing their job and made it even easier for the state to prevent critical or objectionable independent media sources from registration by a complicated procedure of registration and a number of obstacles set in the process. Moreover, the broadened list of prohibited information and ability of the Ministry of Information of the Republic of Belarus to block websites for a period of three months without a court order poses a serious threat to all types of online resources. It is provided that one can be prosecuted for sharing false information, which is rather a vague expression and basically gives the authorities an opportunity to act based on their own interests, often not coinciding with the interests of society.

The most crucial document with regard to the information sphere regulation policy is the national concept of information security dated 18 March 2019. The concept (President.gov.by 2019) highlights an important role of IT technologies in the fulfilment of rights and freedoms of the Belarusian citizens and, at the same time, mentions the challenges to national security posed by the transition to the information society. The state reaffirms its commitment to develop effective and transparent system of governance and introduce ICT into the economic and social sectors and admits the digitisation of economy as the crucial aspect of formation of the information society. In line with that, the state emphasises its dedication to retain information sovereignty, which is not contrary to the

international principles of human rights protection, promotion and fulfilment. Information sovereignty is of paramount importance in light of the fulfilment of the strategy of national security in relation to the raising of awareness on issues such as fake news, cyber-terrorism, the imparting of false information aimed at stirring unrest among society and harming national interests and security. From this perspective, the state deems it necessary to promote critical attitudes toward information and activities that are disrespectful to the national customs, traditions, social morals, rights as well as to enhance intolerance to disinformation, information manipulations and attempts of psychological influence by the information means. In this light, the concept (President.gov.by 2019) underlines the necessity of an increase in the range and volume of the national media sources as well as their efficiency in the population. To support this statement the chart of the state budget expenses on the media development is provided in Table 5.

Table 5: State budget support to mass media in Belarus⁶

Year	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Funding	64 mln. EUR	40 mln. EUR	54 mln. EUR	45,5 mln. EUR	60 mln. EUR	52 mln. EUR	60 mln. EUR	45 mln. EUR	47 mln. EUR	48 mln. EUR	62 mln. EUR

From the chart it is clear that the state authorities are taking steps to satisfy the necessity mentioned above and improve the quality of the national media sources functioning. However, in reality the state's increased budgetary expenses do not constitute attempts at liberalising the national information space but rather implies a dedication to enhance control over it.

In addition, the Concept (President.gov.by 2019) underlines the special place of the information and digital security. The state goes to much trouble to prevent imparting untrue information able to harm the national interest and bring unrest to society by tightening control over the information space within the country and more extensive gathering of users' personal data. These measures reaffirm governmental control over media and other information sources and further decrease anonymity on the internet (Pravo.by 2003). However, at the same time the state confirms its efforts in developing effective instruments of digital security in Belarus and ensuring the safety of users' personal data from unsanctioned access.

Eventually, it may be concluded that the national concept of information security (President.gov.by 2019) can be considered as a thorough and balanced document reflecting the reality prevailing within Belarusian society. Nevertheless, the provisions with regard to the media may be considered overly repressive and in need of overhaul. The national as well as international independent media sources should be able to operate freely and with full access to the official information and freelancing journalists must not be prosecuted for acting in their

6 Source: <https://baj.by/sites/default/files/analytics/files/smi-01572019-en.pdf>.

professional field. This is an essential condition of fulfilment of the freedom of expression, which implies the freedom to receive information from various resources.

Therefore, the following challenges to the full and sustainable implementation of the freedom of expression might be highlighted:

- the extensive intrusion of the government into the functioning of the national media sources;
- the overregulation of the national information space.

In order to overcome these challenges, the government of the Republic of Belarus in cooperation with civil society has to implement the following recommendations:

- to increase activism of the national civil society and human rights NGOs;
- to make the government revise the system of regulation of the information space and media sources;
- to establish the monitoring and self-regulating mechanisms for media in order to identify infringements upon freedom of expression and eliminate them with minimum level of intrusion by the state.

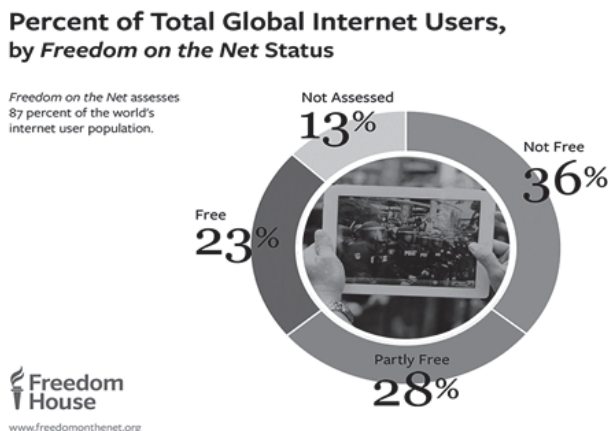
4 New technologies as a tool of protection of human rights: A case study of the Kyrgyz Republic

The case study of the Kyrgyz Republic is an analysis of the legislation, the government electronic services, and the main challenges for the state in the era of global automation. The conclusion of this part recommends the necessary actions to respect, protect and fulfil human rights through new technologies.

4.1 Analysis of national legislation and human rights protection mechanisms in digital space

Kyrgyzstan is a mountainous country in Central Asia with a population of 6 389 500 people as of 1 January 2019. According to the Freedom House Freedom on Net 2018 report Kyrgyzstan is among 28 per cent of countries with partially free internet (Image 1). Kyrgyzstan has 38\100 points in contrast to the neighbouring countries in Central Asia such as Kazakhstan (62\100) and Uzbekistan (75\100), which are among 36 per cent of countries in the category 'Not Free' (Freedom House 2018 (a)).

Image 1: Percentage of total internet users by Freedom on the Net Status



Kyrgyzstan is a developing country. Although digital processes are only beginning to gain momentum, the country aims to move towards becoming a more digital space. To improve the quality of the life of citizens, and to build an open and transparent state, a National Sustainable Development Strategy has been developed, a key component of which is the 'Taza Koom' digital transformation programme. The official launch year was 2016. Since then, it has become clear that the country was not ready for large-scale digital changes. There was no prepared platform and digital infrastructure. Digital infrastructure in Kyrgyzstan is at the medium level. Kyrgyzstan is rapidly increasing the consumption of internet services, especially of international content. However, the quality of telecom-munications and ICT is a major factor in relation to capacity of regional transit bandwidth, independence of national networks, and e-government infrastructure (National 2017).

The legislative level has limited power to regulate the digital environment. The state does not recognise the relations that are exercised in the digital space, making a connection with existing laws and referring to regular and well-known topics and articles in legislation. The Constitution of the Kyrgyz Republic enshrines fundamental rights such as the right to privacy; the protection of honour and dignity; the right to privacy of correspondence (article 29); the right to freedom of thought and opinion (article 31); and the right to freedom of conscience and religion (article 33).

The level of freedom of information is an important criterion in determining the country's compliance with democratic norms. Based on the Constitution the country has various laws related to information. A vivid example of the weak level of regulatory compliance of digital modernisation is the 'Law of the Kyrgyz Republic on guarantees and ways to access information'. This Law regulates the relations that arise in the exercise of the right to freely search, receive, research and produce, transfer and disseminate information, but it is worth noting that this Law

lacks concepts such as internet, digital environment, social networks, and so forth.

Internet resources are not officially recognised media in Kyrgyzstan, but they nevertheless feature in various lawsuits. Jogorku Kenesh (the official name of the country's Parliament) has repeatedly tried to raise the issue of Bills regulating the internet space. It is worth noting that these Bills contain rules that can cause restrictions on freedom of speech on the internet.

The mechanisms for the protection of human rights in the digital environment are not clearly defined. The main elements are written laws and the judicial system. The lack of clear concepts of human rights in the digital environment allows to adjust the letter of the law to the desired meaning. For example, the government agencies by citing anti-extremist law block websites, blogs, and music applications (Freedom House 2018 (A)).

The legislation contains the basics for digitalisation, but remains fragmented and not fully applied. To ensure the protection of rights and freedoms, the Law on the Protection and Use of Personal Data was adopted. Thus, the law equates information on electronic media to paper documents, various electronic transactions to physical transactions, electronic documents and certificates to physical documents, and digital signature to a physical signature.

For the protection of human rights in the digital sphere it is important that the mechanisms could be used. Significant challenges to the implementation of rights are out-dated rules and regulations, gaps in the country's legislation governing the ICT sector, the lack of reliable information and digital infrastructure, as well as weak guarantees in protecting electronic payments, open data and the exchange of personal data.

4.2 The concept of information security in the Kyrgyz Republic: International and regional cooperation

The concept of national security of the Kyrgyz Republic is a system of attitudes, ideas and principles for the protection of individuals, society and the state from external and internal threats to security in all spheres of life. Modern realities prioritise on the concept of security. In this regard information security is one of the most important elements of the concept. According to the Cyber Security Index 2017, Kyrgyzstan ranks 97 out of 180 countries (International 2017).

The Law of the Kyrgyz Republic on Personal Information contains an article on the obligation to provide data transmission via the internet with the necessary means of protection, while maintaining confidentiality of information. Personal data protection should be a priority item in the security concept. At present there is no concept of cybercrime in the law. Government agencies are the main holders of all personal information of citizens. Therefore, they should act as guarantors of the complete protection and security of the personal data. In recent years Kyrgyzstan has witnessed a significant increase in the number of cyber-attacks targeting public and private systems. In 2016 hackers cracked two government agencies: the official website of the State National Security

Committee and the official website of the State Committee on Defense Affairs (Kabar 2016). The hacking of two main bodies that protect personal data indicates weak digital security (Global 2017). The regulatory framework for information security is represented in Kyrgyzstan by documents such as the Constitution of the Kyrgyz Republic, the Civil Code, the Concept of National Security and other laws regulating the security sphere. The country has also developed a Cyber Security Strategy of Kyrgyz Republic 2018-2023. The Cyber Security Strategy was developed with the aim of creating a unified state policy to counter threats in cyberspace and improve the national system of protection of information. The Strategy also confirms the existing gaps in the legislative system and the absence of a cyber security policy.

International cooperation is a significant criterion for the development of states. Joint work aimed at improving human rights and ensuring safe livelihoods has an effect only if there is fruitful work by all states.

As a member country of the Eurasian Economic Union (EAEU), Kyrgyzstan contributes to the improvement of the overall digital space together with neighbouring Kazakhstan, Russia, Armenia and Belarus. The common economic space is not limited to economic relations; the member countries develop their relations in all spheres, one of which is security. Modern challenges render information security in the common space of paramount importance.

EAEU has identified a developmental path related to digital transformation and has developed a Digital Agenda for the implementation period until 2025. To create a durable and secure digital space it is important to develop institutional and legal frameworks. The EAEU Digital Agenda has as its main objective the creation of a safe and independent digital space and the development of the Digital Economy. The transition to a new technical structure taking into account national interests is focused on improving the quality of public services and creating a favourable environment for the development of innovations. While implementing the Digital Agenda, countries may be under a number of security threats, various risks including the loss of digital sovereignty, the emergence of influence and control on national digital space by external players, or the implementation of destructive cyber threats that can be a threat to personal data of states. The cooperation of the participating countries should be based on a coordinated policy of digital transformation. The relationship mechanism should include an open platform for mutual coordination, stimulation and support. The main policy and activity of the EAEU is aimed at the economic component but at the same time the human rights factor is included. The main benefits for human rights in the digital space of the EAEU is that it will serve to improve national digital systems by establishing a common security policy and assist in countering cyber-attacks so as to protect the privacy of citizens and advance economic development.

However, it remains unclear whether participating countries should have a similar legal framework with respect to internet freedom. For example, on 22 March 2019 the President of the Russian Federation introduced the concept of Digital Rights into the Civil Code of the Russian Federation. Does this mean that for equal regulation, member states must have identical laws? Also in the legislation of the Russian Federation there is a Concept for Information Security of Children adopted by a

government decree. On 24 February 2019, the draft law 'On protection of children from information harmful to their health or development' was placed on the official website of the Jogorku Kenesh for public discussion. Public Foundation Legal Clinic 'Adilet' conducted a legal analysis and came to the conclusion that the law contains a number of provisions that carry certain risks to the democratic values of the rule of law including the respect for the observance of the right to freedom of opinion and expression (Public Foundation 2019).

In addition to being a member of the EAEU, the Kyrgyz Republic is also a member of various regional organisations such as the Organisation for Security and Co-operation in Europe (OSCE), the Commonwealth of Independent States (CIS), Shanghai Cooperation Organisation (SCO), and Collective Security Treaty Organisation (CSTO). Each of these structures has developed its own policy aimed at the development of the digital space and the protection of human rights. The main criterion for evaluating the activities of an organisation and unions in this article is the presence of the implementation of the protection of human rights in the digital environment in the activities of the above mentioned organisations.

As the largest security organisation, the OSCE pays special attention to countering cyber threats and ICT security coming from non-state institutions such as organised criminal groups and terrorists, but also provides the basis for preventing states from encroaching on digital sovereignty. Conflicts between states that may arise from the use of ICT can cause a problem. In this regard OSCE member states are working on confidence-building measures.

The confidence-building measures are designed to make cyberspace more predictable and open in this regard to provide important mechanisms, such as: information openness, including discussions of a possible or existing conflict with further escalation, an educational platform, including various educational activities to exchange views, strategies and projects, a security policy that includes collective measures to protect the digital infrastructure, which will contribute to improving the cyber security resilience (Organisation 2016).

There are also other examples of regional cooperation that develop the digital space in different areas:

- (1) The activities of the CIS include the provision of digital integration, the development of a digital economy and the provision of cybersecurity. CIS member states are working on a cybersecurity agreement that will facilitate the rapid exchange of information on new types of information technology crimes, also study digital security threats and propose measures to prevent and curb them.
- (2) The policy of the SCO is aimed at the benefit of the economic and social development of the participating countries. The SCO also covers the digital agenda and carries out its activities related to the development of cooperation, the exchange of information and the transfer of ICT practices. The SCO also considers issues of digital security, interacting in the fight against the proliferation of various crimes, such as terrorism through the internet.
- (3) The CSTO as a military-political bloc carries out its activities directly related to security. The CSTO aims to unite efforts to combat cybercrime, also to create a system of information security and strengthen inter-agency cooperation.

4.3 Development of digital technologies and e-governance in Kyrgyz Republic

Since 2016 Kyrgyzstan has started implementing a Sustainable Development Strategy. Since the beginning of 2018 Kyrgyzstan began to officially launch programmes for the digitalisation of public services. The cardinal change of the state system was met with great optimism of citizens. E-government projects are aimed at increasing state efficiency and counteracting the development of corruption. Examples of different implemented projects include various portals of state agencies, e-visa, e-trading platform, automated border control system e-gates, electronic notaries, and electronic patents.

A bright and successful project that improves the livelihoods of citizens is the system Tunduk. Tunduk is a system of electronic interaction in which ministries, departments, state enterprises, municipal authorities and other organisations (legal entities and individuals) exchange information with each other directly at the machine level. It is important to note its legal value:

- Any transaction passing through the Tunduk platform is automatically signed and becomes a document (certificate, report, information).
- Each state body has its transaction history.
- The transaction is officially signed and it can be used in court as a legal document.
- Any government agency is always aware about a transaction.
- It is impossible to create a fake document as it is automatically created.

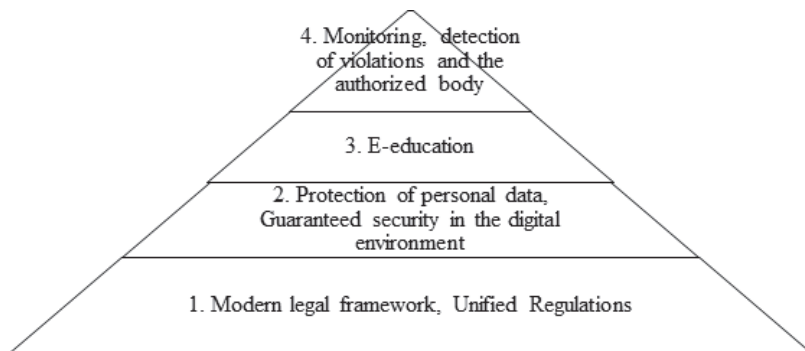
The Tunduk system is based on world practice, namely, the Estonian X-road system. According to specialists the Estonian system allows to save up to €1 billion per year. According to international experts Tunduk will allow the budget to save up to \$300 million per year.

The Tunduk system has as its goal the coverage of a large number of state bodies. At this stage it is possible to identify positive changes in the implementation of E-Gov systems, such as improving the work of state bodies, making public administration more efficient, exchanging information directly, which will reduce the number of illegal documents, and reducing corruption.

4.4 Development of new technologies and protection of human rights: What is next?

To ensure the sustainable presence of human rights in new technologies states are obliged to develop a unified standard for the gradual introduction of the protective mechanism of human rights in the digital environment (Image 3).

Image 2: The pyramid of necessary actions to achieve the sustainability of the presence of human rights in the new technologies



1 *Modern legal framework, Unified Regulations*

Laws that clearly regulate the protection of human rights in the digital environment are required to guarantee the recognition of human rights in the digital environment. Legislation needs to conduct a timely analysis of new digital space challenges. Laws should have the same rules in relation to online and offline rights. Laws should not be duplicated, thereby creating fields for legal gaps helping to avoid legal liability for human rights violations in the digital environment. It is also important to create a sustainable regulatory system from cyber threats. The legal framework should include NGOs, civil society organisations, citizens, and so forth. By involving society forces it can be ensured that the framework does not limit freedom but instead protects human rights.

2 *Protection of personal data, guaranteed security in the digital environment*

Security is an important component in ensuring the protection of human rights in the digital environment. The state must guarantee the enjoyment of human rights in the digital space. The state should provide guaranteed protection of personal data. Need to develop international and regional relations to develop ways to protect cyberspace and improve cyber security.

3 *E-education*

Education is one of the main key components of digital processes. Standards for educational activities and educational regulations should include disciplines that teach important skills, such as digital literacy and digital skills, cyber security, human rights in the digital environment, lessons on the right use of E-Gov services, computer hygiene and other items that will contribute to the safe and proper use of digital services. It is important to introduce important principles through digital processes, highlight human rights and freedoms, contribute to the achievement of the UN SDGs, and so forth.

The example of Estonian digital revolution started in 1996 with the state programme Tiger Leap. This programme was focused on implementing technology education and technology infrastructure at schools.

E-education is an essential part of state development. The educational component of digitalisation must necessarily include projects and research in the field of digital development, information campaigns to reduce digital inequality among citizens and the development of digital censorship and etiquette. An example of a working education mechanism is the Digital Rights School in Kyrgyzstan, which includes in its activities new technologies and digital human rights. E-skills become mandatory selection criteria when applying for a job. Lack of technological skills contributes to increasing the inequality gap (The World Bank Group 2016).

4 *Monitoring, detection of violations and the authorised body*

A component of creating a regulatory framework focused on the digital environment is the creation of a working mechanism, the body authorised to monitor and detect human rights violations in the digital environment. A competent authority is necessary to conduct surveys, focus groups and monitoring in order to identify the causes of inequality, improve access for all categories of citizens, improve the regulatory framework, and identify weaknesses.

5 Conclusions and recommendations

This article explores the dualistic nature of ICT in a way they affect the processes occurring in the world. Based on the case studies of three former CIS countries, it was found that new technologies can significantly contribute to the fulfilment of human rights, and in this process, one of the key roles is assigned to civil society that can properly use those technologies for the achievement of democratic goals. The vivid example of the latter is the digital activism in Armenia that helped different civil society organisations to reach a wider audience and awaken the politicised identity of the major part of the population. Digital activism played a decisive role in mobilising masses and making them exercise their civil and political rights during the Armenian Velvet Revolution. However, in this case one of the challenges that CSOs may encounter on their way is the abuse of state power. Both in Belarus and Kyrgyzstan the states act as opponents for the civil society in the implementation of various activities, thereby infringing on many crucial human rights that citizens should enjoy. Therefore, what has to be done in this case is bringing the authorities and civil society to a dialogue in order to overcome the problem of extensive regulation of all the spheres of society and ensuring the best conditions for the development of a scientifically-progressive digital state.

Another major finding in this article was that the transition towards technologies may have negative impacts such as a lack of control on the content shared online, risk of being subjected to cyberbullying and so forth. Despite the fact that the social media platforms have security measures, a gap remains that allows disinformation to be spread

throughout the world. Another factor leading to the indirect negative impact of new technologies is the lack of media literacy of the wider public. Indeed, it is not the fault of new technologies, rather of the low media literacy level, that the media are being used to manipulate people through new technologies.

Thus, it can be said that as any coin new technologies have two sides: *Tails*, for example, may show how new technologies contribute to the freedom of expression and freedom of speech of people; and *heads* may show how the former may also contribute to the spreading of hatred, discrimination, and cyber bullying.

However, relying on the case studies of Armenia, Belarus, and the Kyrgyz Republic it may be said that the overall sustainable and effective implementation of human rights in the context of rapid integration of new technologies requires the combination of the efforts and responsible approaches of individuals, commercial organisations, civil society, states and international organisations. Comprehensive programmes and individual decisions in the field of the protection and implementation of human rights can provide for the inclusion of a complex mechanism, the key components of which are the political will, a strong legal framework, the presence of relevant institutions, infrastructure and technical environment.

References

- Arminfo (2019) *Samvel Martirosyan: Cyber security of Armenia and Azerbaijan is vulnerable*, available at https://arminfo.info/full_news.php?id=39061&lang=3 (last visited 1 April 2019)
- Artezio 2000 'Belarus among top 20 countries with the best e-government services' 7 February 2018, available at <https://www.artezio.com/pressroom/blog/belarus-among-top-20-countries-best-e-government-services> (last visited 27 February 2019)
- BAJ 2008 'Repressions against journalists in Belarus, 2018 (chart)' 5 September 2018, Belarusian Association of Journalists, available at <https://baj.by/en/analitics/repressions-against-journalists-belarus-2018-chart> (last visited 3 March 2019)
- Belarus.by 2009 'Changes to the law about media sources came into force 1 December 2018', available at https://www.belarus.by/ru/government/documents/osnovnye-izmenenija-v-zakon-o-smi-vstupili-v-silu_i_0000092147.html (last visited 19 March 2019)
- Eurasian Economic Union EAEU, World Bank 2017, *EAEU Digital Agenda 2025: prospects and recommendations*, available at http://www.eurasiancommission.org/ru/act/dmi/SiteAssets/2017.10.04%20%E2%80%9320EAEU_A3fold_ENG_PRINT.pdf (last visited 21 March 2019)
- European Forum for Democracy and Solidarity *Armenia's portfolio* 2018, available at <https://www.europeanforum.net/uploads/countries/pdf/armenia.pdf> (last visited 14 February 2019)
- Fact Investigation Platform 2018 'Vahe Enfiayyan and the army of fake Facebook users from the Prosperous Armenia Party', available at <https://fip.am/en/5378> (last visited 8 April 2019)
- Forumpravo.by 2013 'The Law of the Republic of Belarus about personal data' nd, available at http://forumpravo.by/files/proekt_zakona_o_personalnih_danih.pdf (last visited 3 March 2019)
- Freedom House 2018(a) 'Freedom on net 2018' nd, available at <https://freedomhouse.org/report/freedom-net/2018/kyrgyzstan> (last visited 28 April 2019)
- Freedom House 2018(b) 'Freedom on the Net 2018' nd, available at <https://freedomhouse.org/report/freedom-net/2018/belarus> (last visited 25 March 2019)
- Freedom House 2018(c) 'Freedom on the Net 2018' nd, available at <https://freedomhouse.org/report/freedom-net/2018/armenia> (last visited 15 June 2019)
- Global Cyber Security Capacity Centre 2017 'Cyber Security Capacity Review – Kyrgyz Republic', available at https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/CMM_Kyrgyzstan%20Report%20final_execsummary_1701030.pdf (last visited 20 February 2019)
- Human Rights Watch 2019 'Belarus. Events of 2018' nd, available at <https://www.hrw.org/world-report/2019/country-chapters/belarus> (last visited 5 March 2019)
- International Telecommunication Union 2017 'Global Cybersecurity Index', available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (last visited 1 April 2019)
- IREX 2018 'Media Sustainability Index 2018: The development of sustainable independent media in Europe and Eurasia' available at <https://www.irex.org/sites/default/files/pdf/media-sustainability-index-europe-eurasia-218-full.pdf> (last visited 8 April 2019)

- Kabar 2016 'Kyrgyz security service website hacked', available at <http://old.kabar.kg/eng/society/full/16534> (last visited 15 April 2019)
- Kaspersky Daily 2018 'GetContact: Find a contact or give your contacts away?' available at <https://www.kaspersky.com/blog/getcontact-collects-personal-data/21453/> (last visited 8 April 2019)
- Freedom of Information Centre of Armenia 2011 'Law of the Republic of Armenia on Protection of Personal Data 2015', available at http://www.foi.am/u_files/file/Personaldataprotectionlaw_ENG.pdf (last visited 8 April 2019)
- National Institute for Strategic Studies of the Kyrgyz Republic 2017 'Digital development assessment – Kyrgyzstan, available at http://www.ict.gov.kg/uploads/ckfinder/files/KG_Digital%20Development%20Assessment_Final.pdf (last visited 15 March 2019)
- Organisation for Security and Co-operation in Europe Permanent Council 2016 *Decision No 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from Use of Information and Communication Technologies*, available at <https://www.osce.org/pc/227281?download=true> (last visited 25 March 2019)
- Pravo.by 2003 'The Law of the Republic of Belarus "About the media sources"' 17 July 2008, available at <http://pravo.by/document/?guid=3871&p0=H10800427> (last visited 8 March 2019)
- President.gov.by 2019 'Directive of the Security Council of the Republic of Belarus' 18 March 2019, available at <http://president.gov.by/uploads/documents/2019/1post.pdf> (last visited 18 March 2019)
- Public Foundation Legal Clinic "Adilet" 2019, Analysis of the concept of the draft law of the Kyrgyz Republic "On the Protection of Children from Information Harmful to their Health or Development", available at http://www.adilet.kg/ru/news/full/368?fbclid=IwAR1tqz9v4_IqJWX6iwKZxAlSfc6_yKX-DkuNmBtIA CoG6jhGDGLtwxOZ7fE (last visited 10 March 2019)
- Shubladze R 'Armenian snap elections seen as the final chapter of the Velvet Revolution' 2018, available at <https://europeelects.eu/2018/12/04/armenian-snap-elections-seen-as-the-final-chapter-of-he-velvet-revolution/> (last visited 1 April 2019)
- The World Bank Group 2016 'Digital Development Report 2016. Digital Dividends', available at <http://pubdocs.worldbank.org/en/961361455690144451/Presentation-WDR2016-Overview-Zahid-Hasnain-en.pdf> (last visited 23 March 2019)
- United Nations Office on Drugs and Crime 2019 'Criminal Code of the Republic of Armenia 2003', available at https://www.unodc.org/res/cld/document/armenia_criminal_code_html/Armenia_Criminal_Code_of_the_Republic_of_Armenia_2009.pdf (last visited 14 March 2019)

Selected developments in human rights and democracy in 2018: Migration and asylum in Europe

Lorenzo Durante Viola,* Cristina Pugnale,**

Federica Russo,* Tamara Siwczyk**** and**

Paloma Torres Lopez*****

Abstract: 2018 marks a milestone year with respect to the socio-legal and political aspects surrounding the issue of migration due to the adoption of the two Global Compacts (the Global Compact on Refugees and the Global Compact on Safe, Orderly and Regular Migration). In the first part this article gives an insight into the content of the Global Compact on Migration (GCM), which led to a loss of unity of European Union representation. The article further analyses two highly controversial topics from the Global Compact, namely, the so-called 'climate migrants' and 'migrants in vulnerable situations'. Notwithstanding its soft law nature, the examination of the GCM reveals that both groups received recognition at a global level for the first time. Furthermore, the article analyses how these divergent positions on migration are being reflected in the EU's policy making. The article finds that, instead of lifting the unequal migratory burden from some member states through harmonisation, EU policies have had the main aim to prevent migrants from entering into EU jurisdiction. Crucial developments in this context are the criminalisation of search and rescue NGOs, the transfer of search and rescue responsibilities to third countries and the outsourcing of migration-related responsibilities. Overall, the lack of progress in reforming the common European asylum system resulted in the externalisation of the EU migration policies through bilateral and multilateral agreements with transit countries. Finally, although the issue of migration requires political responses, the protection of refugees and migrants has increasingly relied upon judicial institutions.

* BA in International Studies (University of Trento); MA in European Studies (Université Libre de Bruxelles); MA in Human Rights and Democratisation (EIUC/Global Campus of Human Rights); Trainee at the Office of the European Union Special Representative for Human Rights, Mr Eamon Gilmore; lore.durante@gmail.com

** BA in International Diplomatic Sciences (University of Trieste); MA in Human Rights and Democratisation (EIUC/Global Campus of Human Rights); Human Rights Trainee at European Network of National Human Rights Institutions (ENNHRI); cris.pugnale.cp@gmail.com

*** Master Degree in Law (Federico II of Naples University); MA in Human Rights and Democratisation (EIUC/Global Campus of Human Rights); Legal Advisor for asylum seekers and migrants (Marseille); federica.russo.m@gmail.com

**** Magistra Iuris in Law (University of Vienna), MA in Human Rights and Democratisation (EIUC/Global Campus of Human Rights); Legal Counsellor for asylum seekers at Verein Menschenrechte Österreich; tamara.siwczyk@gmail.com

***** LLM (Universidad Pontificia Comillas); MA in Human Rights and Democratisation (EIUC/Global Campus for Human Rights); Children on the move Protection Officer at Save the Children and Associate Professor at Universidad Pontificia Comillas; palomatorreslopez@gmail.com

Key words: *Global Compact on Migration; climate migrants; migrants in vulnerable situations; search and rescue; externalisation policies; common European asylum system*

1 Introduction

In 2000 a high-profile smuggling incident caused the death of 58 migrants who, after a long journey through several countries – including three European Union (EU) member states – suffocated in the back of a truck. Their bodies were found in the British harbour of Dover. Similarly, on 23 October 2019 39 migrants were found frozen to death in the back of a refrigerated lorry in East England. Today, like 20 years ago, people seeking safer havens and better living conditions are still dying at the EU's external borders. Despite some positive developments, these episodes basically reflect the EU and its member states' longstanding failure to comprehensively address migration and refugee protection as an inherently global and transnational phenomenon.

The year 2018 is likely to go down in history as a milestone year for its great potential impact on migration-related issues. The Global Compact on Migration, the first soft law instrument to address migration globally and comprehensively, was adopted by the international community in December 2018 bringing new challenges to the attention of the international community. Simultaneously, the EU and its member states have continued developing new controversial migration and asylum policies in an attempt to address the main migration issues with which southern member states are regularly confronted.

This article critically analyses such major developments with a special focus on those areas that were disproportionately affected by migrant inflows in 2018, namely, the southern EU member states. The first part presents the Global Compact on Migration (GCM) and two of its most controversial outcomes, namely, the concept of 'climate migrants' and the notion of 'migrants in vulnerable situations'. In addition it sheds light on the EU member states' contradicting stances regarding the adoption of the GCM. Hence the article examines the issue of the loss of unity of the EU throughout the negotiation process. The second part assesses the main developments that hinder an agreement on a common EU approach to migration and asylum policies such as search and rescue and the externalisation of borders and migration management to third countries. In addition, recent case law of the EU and member states on legal responsibility for migration-related human rights violations is briefly addressed. The conclusion highlights the transversal connections between the selected developments.

2 The Global Compact on Safe, Orderly and Regular Migration: The stance of the European Union

The adoption of the United Nations (UN) Global Compacts on Migration and Refugees is one of the latest major migration-related developments and will help make the year 2018 go down in history as a milestone with regard to the protection of refugees and migrants (UNGA 2018). The process leading to the elaboration and adoption of the two Global

Compacts was set in motion by Annex I and II of the 2016 New York Declaration for Refugees and Migrants which, for the first time, brought together the international community to discuss the impelling need to jointly and comprehensively address migration (IOM 2018). The New York Declaration, adopted by all 193 UN member states, is a political declaration establishing a set of commitments upon which the Global Compact on Migration (GCM) builds. Unlike its counterpart on refugees, the GCM was more controversial and, for the different reasons analysed below, raised much concern and opposition from several state delegations.

The GCM is a 'non-legally binding, cooperative framework' (para 7) which lays down 23 main objectives reflecting commitments and a range of actions (policy instruments and best practices), as well as guidelines for implementation, and follow-up and review mechanisms (UNGA 2018). The main fundamental idea behind the GCM is that '[m]igration ... is a source of prosperity, innovation and sustainable development' (para 8) but, because of the inherent transnational nature of human mobility, it is not possible for a country to 'address the challenges and opportunities of this global phenomenon on its own' (para 11) (UNGA 2018).

After almost two years of intergovernmental negotiations and consultations, the GCM was eventually adopted by 152 UN member states in Marrakesh, Morocco, on 10 December 2018. Yet, a significant number of states withdrew from the final phase of negotiations – an important factor that cannot be underestimated.

In this part, the article analyses such unfortunate developments with a special focus on the European regional level. The most controversial aspects of the Compact, namely, the GCM's inclusion of climate migrants and the new concept of 'migrants in vulnerable situations', will in particular be analysed. This functions to introduce some points that raised the concern of several participating member states. A specific national case will be considered in order to present more in depth the main arguments EU member states put forward against the Compact. In this sense, the Italian case is believed to be particularly relevant to the purpose of the article and sufficiently representative of various reasons behind member states' opposition to the GCM.

2.1 Shedding light on the nexus between climate change and migration

According to the IOM and IDMC, 17,2 million new displacements took place due to disasters and 764 000 people were displaced due to drought in 2018 alone (Ionesco 2019). At the same time, the year 2018 has marked an important year for the development of the protection and visibility of persons affected by natural disasters and the adverse effects of climate change.

As noted, the New York Declaration resulted in the adoption of two milestone global compacts, one of which was the GCM adopted in December 2018 (Piper 2018: 323). Although the GCM's main objective is to address the drivers of migration, some states argued against the inclusion of the issue of climate migrants in the Compact. In any event, climate-related migration was included in the final instrument, and for the first time the nexus between the adverse effects of climate change and migration (the so-called disaster-migration nexus) was recognised on a global multilateral level (Kálin 2018: 665).

The GCM acknowledges that people may be forced to migrate due to either sudden natural disasters or slow-onset processes that result in the uninhabitability of their homes. Some scholars argue that the term 'refugee' should not be applicable to 'climate migrants' in these situations because it exclusively means persons seeking refuge. In this regard it should be noted that the Refugee Convention of 1951 grants legal protection to persons that are being persecuted for reasons of race, religion, nationality, membership of a social group or political opinion, without including displacement in the context of environmental factors. The IOM and several other scholars prefer the term 'climate migrants' since it is able to cover not only cases in which people are forced to leave their homes immediately but also cases in which migration occurs at the early stages of slow-onset climate change effects (Behrman 2018: 6).

The GCM further enshrines the commitment of states to strengthen resilience and prevent displacement as a first step, but also to develop disaster preparedness strategies and to ensure access to humanitarian assistance. However, the crucial objective of the Compact is to enhance and facilitate regular migration pathways when people are forced to migrate (Kälin 2018: 666). When these people migrate not only internally but are displaced across borders, they will require international protection either temporarily or permanently (Kälin 2018: 664).

Furthermore, it is crucial to bear in mind that climate migration is a highly complex, heterogeneous and, most importantly, multi-causal phenomenon. According to the Refugee Convention, in order to be granted asylum, the applicant is required to flee due to the fear of persecution for *one* of the above-mentioned reasons. Yet, climate change-related mobility can be multi-causal. For example, a drought in a war-torn and failed state such as Somalia will affect its citizens differently than a drought in a country in the global north (Pilkey 2016: 129). Therefore, the reasons for leaving one's home country according to climate change can consist of multiple factors, such as a combination of drought and poverty or other vulnerability-related factors.

While the GCM has shed light on a topic that was in urgent need of being addressed, some human rights defenders condemned the soft law nature of the Global Compact. Nevertheless, the GCM could become the ground on which binding law may be interpreted or created in any follow-up process. Paradoxically, this was also an argument advanced by states for withdrawing from voting for the Compact, since many state representatives argued that they wanted to foreclose the possibility of being legally bound on the basis of customary law, which can be developed through soft law (Gammeltoft-Hansen 2017: 9).

It appears that the GCM's recognition of the nexus between migration and the adverse effects of climate change is a step in the right direction, but nevertheless more needs to be done and sooner than later.

2.2 Migrants and refugees: An out of date dichotomy? The concept of 'migrants in vulnerable situations' in the GCM

The GCM and the Refugee Compact are the result of simultaneous but

separate processes.¹ Moreover, while the Refugee Compact was drawn upon the well-established body of international refugee law, the GCM could not rely on an equally solid legal framework. Indeed, even though migrants are entitled to a wide range of existing rights and human rights protections irrespective of their administrative status, migration had never before been comprehensively and globally addressed by the international community (McAdam 2018: 573). In this sense, the GCM constitutes an unprecedented effort at the global level to develop a comprehensive response to a phenomenon as complex as human mobility. The Preamble to the GCM explicitly acknowledges the importance of this instrument by affirming that the GCM 'is a milestone in the history of the global dialogue and international cooperation on migration' (UNGA 2018: para 6).

The first international document to explicitly question the traditional dichotomy between refugees and migrants is the GCM's predecessor, the New York Declaration for Refugees and Migrants (UNGA 2016a). The New York Declaration first affirms that all refugees and migrants are rights holders, regardless of their administrative status. Then, the Declaration makes clear that '[t]hrough their treatment is governed by separate legal frameworks, refugees and migrants have the same universal rights and fundamental freedoms' (UNGA 2016a: para 6). Most importantly, it acknowledges that refugees and migrants 'face many common challenges and have similar vulnerabilities, including in the context of large movements' (UNGA 2016a: para 6). The concept of 'migrants in vulnerable situations' had recently been developed at the UN level and was fully endorsed by the New York Declaration. This doctrine intended to protect the human rights of those migrants in vulnerable situations falling outside the legal category of refugees and, therefore, the scope of application of international refugee law.

Overall, the GCM accords with the New York Declaration's approach but adopts a more subtle wording likely to accommodate UN member states' concerns. While acknowledging the existence of the same rights and fundamental freedoms for both migrants and refugees, the GCM emphasises that 'migrants and refugees are distinct groups governed by separate legal frameworks' and that '[o]nly refugees are entitled to the specific international protection defined by international refugee law' (UNGA 2018: para 4). Thus, the New York Declaration and the GCM contain substantially similar provisions, which differ slightly from a more formal perspective.

The vulnerability of migrants other than refugees and their equal need for protection was ultimately among the most contested points of the GCM's negotiation phase. Similarly, the purported equivalence of migrants and refugees in the GCM was a common argument put forward by member states in their opposition. Yet, as was demonstrated above, the GCM's wording clearly differentiates migrants from refugees, rebutting this assertion. In addition, the elaboration of two separate compacts setting up 'complementary international cooperation frameworks that fulfil their respective mandates' (para 3) aligns with the existing international legal framework and dominant understanding of migration, which places

1 The drafting of the GCM was state-led while the Refugee Compact was facilitated and coordinated by the UN High Commissioner for Refugees (UNHCR).

refugees on one side and the broader category of migrants on the other (UNGA 2018).

2.3 The role and position of the European Union: Why has the European Union lost its unity of representation before the Global Compact?

As the UN Modalities Resolutions on the intergovernmental negotiations makes clear, the process of negotiations and consultations culminating in the adoption of the GCM was meant to be open, transparent, participative and inclusive (UNGA 2017). In particular, according to the UN document, the consultations would include regional groups (paras 5, 17) and examine 'regional and sub-regional aspects of international migration' (para 22(a)) (UNGA 2017). All relevant stakeholders were encouraged to contribute throughout the entire preparatory process through the 'participation in global, regional and sub-regional platforms' (para 7), as well as 'regional and sub-regional consultative processes' (para 22 (b)) (UNGA 2017). Therefore, as a major regional organisation, the EU had the opportunity to play an important role during the preparatory process of the GCM.

The EU mainly participated in the GCM negotiation process 'through the delivery of EU statements by the Union delegation at the UN', as provided by article 221 of the Treaty on the Functioning of the European Union (TFEU) (Melin 2019: 195, 203). Within the EU, however, the institutional organ leading the negotiation and drafting phase on behalf of EU member states was the European Commission pursuant to article 17 of the TFEU. This provision establishes that the Commission shall be responsible for the EU's external representation, with the exception of the common foreign and security policy. Yet, the growing discontent with the GCM by a considerable number of EU member states raises the legitimate question of whether the Commission could credibly ensure the unity of EU representation before the UN community of states.

Until May 2018 all EU member states, except Hungary, had actively participated in the consultation and negotiation process.² Given its government's long-standing anti-immigration position, Hungary's withdrawal from the negotiations did not come as a surprise. Hungary, however, was only the first of a long line of member states that abandoned the negotiations. Between July and November 2018, seven other member states withheld their endorsement of the GCM: Austria, Bulgaria, Czech Republic, Poland, Latvia, Romania and Italy. Additionally, the adoption of the GCM caused heated political debates in several other member states, such as Germany, France, Croatia, Estonia, The Netherlands, Slovenia and Belgium. In Belgium disputes over the GCM led to a virulent political crisis and the resignation of the Belgian Prime Minister, Charles Michel.

The potential of so many dissenting opinions to undermine the unity of EU representation and the European Commission's role is clear for a number of reasons. First, the TFEU establishes important principles that should guide member states in their actions and practices, irrespective of their potentially temporary political posturing. According to articles 4(3)

2 This clearly emerges from an EU Statement issued in May 2018 on behalf of 27 EU MSs during the GCM's fourth round of negotiations (EU Statement 2018).

and 34(1) of the TFEU, member states are obliged to coordinate their actions in international organisations and at international conferences pursuant, among others, to the principle of sincere cooperation. Accordingly, member states should uphold or at least refrain from contradicting the EU's agreed-upon common stance. In this regard, the fact that such a common position was agreed upon in Brussels behind closed doors and the lack of transparency that accompanied this make it difficult to determine whether any actual internal coordination resulted from a mutual agreement among all member states (Melin 2019: 207). In any event, the sudden withdrawal from the GCM by some member states seems to have resulted in a violation of the principle of sincere cooperation. For instance, the decision of the Austrian government, which was then holding the EU Council Presidency to withhold its support to the GCM, caused harsh reactions and has been criticised for failing to fit into its leading institutional role. Although in the last phase of negotiations the Commission was officially acting only 'on behalf of 27 member states thereby excluding the position of Hungary' (Melin 2019: 203), the subsequent withdrawal of such a considerable number of EU member states had inevitably undermined the role of the Commission and made the EU lose its unity of representation before the GCM.

The UN Modalities Resolution also demanded the effective participation of parliaments (UNGA 2017: paras 6, 8, 30). In this sense, the European Parliament is a major human rights actor within the EU system, and has since 2000 been pushing for a more comprehensive and holistic approach to migration.³ In 2014 the European Parliament adopted a resolution 'on the situation in the Mediterranean and the need for a holistic EU approach to migration' (EP 2014). Finally, with another resolution in April 2018, the EP took a strong public stance by openly and fully embracing the GCM, its objectives, commitments and follow-up mechanisms (EP 2018).

Finally, this part analyses the stance of Italy which, as in the case of most of the other leavers, demonstrated support for the GCM until a very late phase of the negotiation process. In September 2018 the Italian Prime Minister, Giuseppe Conte, delivered a speech before the UN General Assembly where he clearly expressed Italy's support to the GCM. However, only two months later, before the virulent opposition from his government's right-wing political party, Conte referred the decision concerning the GCM's endorsement to the Italian Parliament which eventually rejected it.

Italy's main arguments against the Compact include the alleged introduction of a human right to migrate; the lack of a clear distinction between regular and irregular migration and between refugees and migrants; the establishment of new obligations for states capable to undermine their national sovereignty; and the likely increase in migration flows the Compact's endorsement would purportedly cause. These arguments can easily be dismantled by only a cursory reading of the GCM's text. First, the Compact rests on existing international frameworks and human rights standards and due to its non-binding nature cannot

3 In 2000, during the drafting process of the EU's anti-smuggling legislation, the so-called Facilitators Package, the European Parliament affirmed that '[a] common immigration and asylum policy for the Member States can only be efficient if it is comprehensive and covers all essential means of obtaining admittance' (LIBE 2000).

create new obligations on states. Second, there is no such mention of a new right to migrate and of a state's duty to receive migrants. By contrast, the GCM explicitly upholds states' national sovereignty while determining their migration policies (UNGA 2018: para 15(c)). Moreover, as demonstrated above, the existence of two separate instruments dealing with refugees and migrants respectively clearly retains the traditional dichotomy between migrants and refugees.

The majority of the other leavers used arguments similar to those of Italy while justifying either their abstention or direct opposition to the Compact. The former Commission president, Jean-Claude Juncker, while commenting on the increasing number of EU member states abandoning the Compact, stated that 'those countries that decided they are leaving the UN migration compact, had they read it, they would not have done it. [This] gives you the idea that many people do not actually know what is in there' (Carrera 2018: 2). The UN Special Representative for International Migration, Louise Arbour, also harshly condemned the leavers' decision by affirming that this 'reflects very poorly on those who participated in negotiations ... it's very disappointing to see that kind of reversal so shortly after a text was agreed upon' (Carrera 2018: 2).

2.4 Concluding remarks

It may be argued that the elaboration of the Global Compacts on Migration and Refugees led the international community to take important steps forward but, at the same time, this process also confirmed the reluctance of states to progressively address issues as delicate as migration and border management.

Overall, the crucial significance of the GCM lies in the acknowledgment of the causal link between climate change and the fact that people migrate out of their home countries due to its inhabitability. Despite its soft law nature, the GCM can still have a norm-filling and interpretative role, but most importantly it constitutes the first legal step to tackle the issue of climate change-related migration for the future. Also, a (timid) step towards the extension of protection to migrants other than refugees is remarkable from a human rights perspective.

It nevertheless remains unfortunate that the EU was not able to keep a united stance when upholding the Global Compact on Migration. While the UN Modalities Resolutions had pushed for the effective participation of parliaments, at the European level the European Parliament does not seem to have had a strong voice during the negotiations. Despite the European Parliament's open support for the GCM, eventually five EU member states abstained from voting (Austria, Bulgaria, Italy, Latvia and Romania), while three member states were firmly opposed to the GCM (Czech Republic, Hungary and Poland). Although it is not clear to what extent all EU member states could initially display their position around the GCM, the leavers' behaviour could allegedly result in the violation of the principle of sincere cooperation enshrined in the TFEU. Finally, considering the superficial and fatuous arguments on which the leavers justified their positions and the impelling need to globally and comprehensively address migration, the recalcitrance of member states is alarming and demonstrates their potential to undermine the effective impact of the GCM in Europe.

3 Migration and asylum in Southern Europe: Stuck between inter-governmental politics and European Union policy making

The controversial tension between the EU and its member states in relation to their position towards migration analysed in the previous part is also reflected in the EU's own migration policy. With the so-called 'migration crisis' of 2015, the Common European Asylum System (CEAS) proved obsolete in addressing the substantially changed nature of migration flows. Consequently, in the 2015 European Agenda on Migration, the European Commission highlighted the need to move from a system disproportionately affecting frontline member states and encouraging secondary movements towards a fairer system in order to ensure the equal sharing of responsibility (Tsirogianni 2018: 13).

Although the general perception is that the negotiations for the CEAS reform launched in 2016 have been deadlocked, five of the seven proposals at stake have reached the trilogue negotiations between the European Parliament and the Council (Pollet 2019). However, the inability to reach an agreement on the reform of the Dublin Regulation, particularly regarding the criteria for the identification of the EU member state responsible for examining an asylum application and provisions such as 'safe third country', border procedures and solidarity, keeps the whole EU asylum *acquis* blocked (Nicolosi 2019). Meanwhile, member states supported by the EU have focused on keeping migrants away from their borders by implementing externalisation policies through agreements with transit third countries (Frelick 2016: 206), stepping up border security and dismantling search and rescue (Fine 2019: 8).

In this vein, the June 2018 European Council was expected to be 'the last chance to resolve the deadlock on the solidarity chapter of the Commission's proposal for a Dublin IV Regulation' (ECRE 2018: 3) and finally have the package adopted before the May 2019 European Parliament elections. However, the meeting was overshadowed by the need to address the Italian government's refusal to allow the disembarkation of migrants and Malta's ban on non-governmental organisations (NGOs) to operate at sea (ECRE 2018: 4). Far from giving the final push for the CEAS reform, the Council proposed two new concepts, namely, 'controlled centres' and 'regional disembarkation platforms' (European Council 2018b: para 5), which represents 'a new addition to the externalisation toolkit' which will be analysed below.

This part addresses the most relevant developments that took place throughout 2018 in the field of EU migration and asylum policies that have been – and still are – the main obstacles to a move towards a common EU approach based on human rights, solidarity and accountability. The first part focuses on Search and Rescue and particularly on the implementation of policies aimed at criminalising search and rescue NGOs, restricting European search and rescue capacities and transferring search and rescue responsibilities to third countries. The second part critically examines further developments on externalisation policies adopted by the EU and its member states in order to limit the arrival of migrants and outsourcing their migration-related responsibilities. Finally, legal developments regarding the responsibility of the EU and member states are considered in light of recent case law and cases pending before regional and international courts.

3.1 The shrinking space of search and rescue in the Mediterranean

Search and rescue in the Central Mediterranean has for some time been a matter of dispute among Southern EU member states. The disagreement has mainly concerned the nature and scope of obligations under international maritime, refugee and human rights law and has primarily involved Italy and Malta, due to their different interpretations of the 'place of safety' concept and the overlap of their respective search and rescue regions (Trevisanut 2010). In recent years the changing geopolitical context and the increased inflow of migrants from the Mediterranean Sea have substantially transformed the framework in which search and rescue takes place (Cuttitta 2018).

The developments analysed below, namely, the criminalisation of search and rescue NGOs, the disengagement of the EU and its member states from search and rescue and the shifting of search and rescue responsibilities to Libya, have to be seen in the context of a 'broader strategy of *contained-mobility*', that is, aimed at 'detering, limiting and filtering asylum seekers' movements at different stages of their various mobility trajectories' (Carrera 2019b: 9). In this regard, serious concerns have been raised about compliance by the EU and member states with their obligations under international law, the European Convention on Human Rights (European Convention), but also EU law and national constitutions.

A major turn concerning the search and rescue operational framework relates to the March 2018 Italian elections, which resulted in the leader of the far-right League party, Matteo Salvini, becoming Interior Minister. Salvini pledged to completely stop the inflow of migrants from the Central Mediterranean. A crucial component of his tactic was to ban search and rescue NGOs, accused (without evidence) of being complicit with smuggling networks,⁴ from entering Italian territorial waters. The NGO-operated Aquarius vessel was the first to be affected by the resulting so-called 'closed ports' policy. After rescuing 629 migrants in distress at sea, on 10 June 2018 the Aquarius was denied entry into Italian territorial waters by Interior Minister Salvini, who argued that Malta should take responsibility (SOS Mediterranée 2018). The diplomatic and operational impasse resulted in the prolonged accommodation of the rescued persons on board of the vessel in international waters, which was only resolved when the Spanish government allowed disembarkation in Spain (Fernandez & Rubio 2018).

Several similar cases followed, often resulting in extra-EU treaties 'disembarkation and relocation arrangements', that is, inter-governmental agreements identifying a disembarkation port and a relocation scheme for the rescued migrants among EU member states participating on a voluntary basis (Carrera 2019b: 23-30). The European Commission and EU agencies, namely, Frontex and EASO, started to become directly involved in such arrangements since early 2019 by identifying member states willing to participate, facilitating inter-governmental dialogues and

4 Such allegations, instrumentally taken up by Italian and European political parties for electoral purposes, were initially made by the EU border agency Frontex (*Financial Times* 2016) and the Public Prosecutor of Catania, Carmelo Zuccaro (Comitato parlamentare di controllo sull'attuazione dell'Accordo di Schengen, di vigilanza sull'attività di Europol, di controllo e vigilanza in materia di immigrazione 2017).

providing operational support at specific steps of relocation procedures (Council of the EU 2019; Carrera 2019b: 25-28).

Meanwhile, search and rescue NGOs have come under increased scrutiny by law enforcement authorities upon politically-driven ministerial orders (Ministero dell'Interno 2019),⁵ often resulting in the seizure of vessels and the prosecution of shipmasters and NGOs' representatives on account of favouring illegal immigration and violating the prohibition of entering territorial waters (FRA 2019).⁶

The criminalisation of civil society actors involved in search and rescue was facilitated by the 2017 Italian government's imposition of a controversial non-legally binding 'code of conduct' upon all search and rescue NGOs operating in the Central Mediterranean (Ministero dell'Interno 2017). Such criminalisation reached a peak on 14 June 2019, when the Italian government adopted the so-called 'Security decree bis', introducing administrative fines from €10 000 to €50 000 for those NGOs' ship masters and ship owners who disregarded a prohibition on entering territorial waters (Art 2 DL n 53/2019). These developments, clearly at odds with the UN Declaration on Human Rights Defenders (UNGA 2016b), have raised serious concerns among humanitarian actors to the extent that in May 2019 five UN Special Procedures of the Human Rights Council sent a joint letter urging the Italian government to refrain from criminalising civil society organisations involved in search and rescue, to withdraw the criminalising decree and to respect their human rights obligations (OHCHR 2019).

The criminalisation of search and rescue NGOs, however, is not specific to Italy. Despite the lack of media attention, Spain and Greece have also adopted similar approaches. Spain, for instance, has stopped granting ship departure permits since January 2019 and threatened the Spanish NGO *Proactiva Open Arms* with a €900 000 fine (Fine 2019: 7). As for Greece, the European Court of Human Rights (European Court) is confronted with an opportunity 'to condemn the growing trend in Greece and Europe of criminalising solidarity' after the complete acquittal of the applicant, namely, the founder of the NGO *Sea-Eye*, by Greek courts who arbitrarily prosecuted him and exposed him to ten years' imprisonment, 'only to suspend his life-saving activities' (GLAN 2019).

In parallel to criminalising search and rescue NGOs, the EU and member states have increasingly disengaged from their search and rescue responsibilities. EUNAVFOR-MED Operation Sophia, a military operation launched in 2015 aimed at disrupting criminal smuggling and trafficking networks in the Central Mediterranean, has been increasingly scaled down, to the extent that in March 2019, despite a six-month extension of its mandate, it was deprived of its naval means and thus of its search and rescue capabilities (ECRE 2019). Similarly, the mandate of Frontex Joint Operation Themis, which replaced Operation Triton in 2018, was also redefined and limited to the Italian search and rescue regions, leaving the Maltese search and rescue regions uncovered (Frontex 2018).

5 One of the most recent ministerial orders concerned the *Mare Jonio* vessel, operated by the NGO *Mediterranea – Saving Humans* (Ministero dell'Interno 2019).

6 None of these prosecutions however have led to a conviction (EU Fundamental Rights Agency 2019).

Italian authorities, which since the 2013 Mare Nostrum operation had taken responsibility over search and rescue operations immediately off the Libyan territorial waters, have progressively transferred these responsibilities to Libyan authorities. This was possible thanks to the Italian and EU support to Libya aimed at preventing migrants from leaving the country, disingenuously presented as part of a 'migration management' strategy designed to prevent deaths at sea and countering smuggling networks.⁷ The partnership with Libya has consisted of financial, material and operational support by both Italy and the EU, aimed at strengthening the capacities of the Libyan Coast Guard (Carrera 2019b: 18). Such support allowed the Libyan interim government to declare a Libyan search and rescue region, validated by the International Maritime Organisation (IMO) in June 2018 (Euronews 2018).

This policy is patently illegitimate as it triggers the violation of fundamental principles of international and human rights law, including most notably the principle of *non-refoulement*.⁸ This policy in fact has translated into the practice of 'pull-backs', that is, the transfer of migrants rescued by the Libyan Coast Guard to migrants' detention centres in Libyan territory, where they have no access to asylum procedures and are held in inhumane conditions, with a well-documented risk of being subjected to serious violations of basic human rights, including torture, sexual violence, slavery and death (OHCHR and UNSMIL 2018).

Furthermore, the Libyan Coast Guard has reportedly adopted, within search and rescue operations, practices that violate international and human rights law, including intimidation and aggression (Cuttitta 2018). A major incident occurred on 6 November 2017, when both the Libyan Coast Guard and the NGO-operated Sea-Watch III vessel were involved in a search and rescue operation (SEA-watch). Witnessed by Italian navy helicopters that were flying over the area, the incident resulted in the drowning of more than 20 migrants and the 'pull-back' of 47 others, later detained in inhuman conditions and subjected to torture and sexual violence. A group of academics and NGOs filed an application against Italy to the European Court of Human Rights, based on evidence provided by a London-based forensic agency (GLAN 2018).⁹ The GLAN-ASGI case is pending and may ultimately become a landmark ruling on the issue of state responsibility (see part 3.3.).

The case of Spain is also controversial. In order to limit search and rescue responsibility, Spain has cut off funds and human resources, and ceded more ground to Morocco by limiting Spanish search and rescue operations and promoting Moroccan authorities to operate in Spanish search and rescue areas, which raises serious human rights concerns among civil society (Neidhardt 2019: 10).

7 These policies in fact have resulted in an increase in deaths per arrivals, although deaths have diminished in absolute numbers (Carrera 2019b: 5-6).

8 The principle of *non-refoulement* is enshrined in multiple legal instruments, including most notably in the 1951 Convention Relating to the Status of Refugees (Art 33(1)), the European Convention (stemming from arts 2 and 3, as developed in the jurisprudence of the European Court), and the EU Charter of Fundamental Rights (art 19).

9 The case was brought to the European Court by the Global Legal Action Network (GLAN) and the Italian Association for Migration Legal Studies (ASGI).

The political and legal unsustainability of the situation led to exploring new solutions in the attempt to comply with search and rescue obligations, on the one hand, without overlooking border states' claims. With this aim, in early 2018 the EU started to explore two highly controversial concepts. The June 2018 European Council invited the Commission and the Council, in cooperation with third countries, the IOM and UNHCR, to work on a proposal about so-called 'regional disembarkation platforms' and 'controlled centres' (respectively centres based in third countries where migrants would be brought after being rescued at sea for the processing of protection claims, and institutionalised and expanded hot spots or, in other words, quasi-detention facilities in the territory of EU member states) (European Council 2018).

The idea of 'regional disembarkation platforms' has been widely criticised due to the impossibility of ensuring respect for international and EU law by the third countries concerned, including in particular the principle of *non-refoulement* and the access to asylum procedures (and reception conditions) that would meet the minimum legal standards. A joint communication issued by UN Special Procedures warned the EU that '[o]utsourcing responsibility of disembarkation to third countries ... only increases the risk of *refoulement* and other human rights violations' (OHCHR 2018b: 2). The African Union (AU) itself has recently discouraged African states to cooperate with the EU on such a proposal, as this would result in the establishment of *de facto* detention centres (Carrera 2019b: 23; Boffey 2019).

'Controlled centres' in EU territory are extremely problematic also because they result in a further institutionalisation of arbitrary detention and other human rights abuses, in particular in light of the well-documented evidence of quasi-detention practices, the forced fingerprinting of individuals, the degrading reception conditions and discriminatory interviewing within the already functioning hot spots (ECRE 2016; Danish Refugee Council 2019). In the absence of a new regulation on relocation based on equal solidarity among member states, however, Southern European member states have given the assurance that they will not allow the establishment of 'controlled centres' within their territory (ECRE 2018a: 3).

In this controversial context, the 23 September 2019 informal summit between Italy, Malta, France and Germany has been seen as a 'milestone' in the controversy over search and rescue and disembarkation (Carrera 2019a: 3). The outcome was a non-binding joint declaration of intent, the Malta Declaration, on a 'controlled emergency procedure' which proposes 'an alternative place or port of safety for disembarking rescued migrants, different from the MS that would otherwise be responsible' (Carrera 2019a: 4), heavily challenging the criteria established by Dublin Regulation. Welcomed by some NGOs, the proposal has been strongly rejected by countries such as Spain and Greece.

3.2 The 'externalisation toolkit'

The developments regarding search and rescue and relocation accord with the outsourcing of responsibility regarding migration and asylum management the EU and its member states have in recent years been promoting. Externalisation policies consist of measures aimed at preventing migrants from entering EU member states' jurisdiction. They

are based on arrangements with allegedly 'safe' third countries aiming at strengthening their border control capacities, 'pulling back' persons intercepted at sea and readmitting migrants (both nationals and non-nationals) into their territory. By avoiding contact with migrants or by applying the 'safe third country' or 'first country of asylum' concepts (that is, by sending migrants back to third countries in which they allegedly can seek asylum, without fully examining their protection needs (ECRE 2017a: 1), EU member states try to avoid legal responsibility particularly with respect to asylum procedures.

The EU has actively promoted externalisation policies, including by adopting financial instruments and directly seeking political arrangements with third countries. The EU Emergency Trust Fund for Africa (EUTFa) has been largely utilised to enhance key African countries' border management capacities in order to contain departures towards Europe (European Commission 2018a). The 2016 EU-Turkey agreement, aimed at reducing irregular migrants' departures towards – and to facilitate their return from – Greece is presented as a model for 'good' migration management (European Council 2016a; European Council 2018). In 2017 the memorandum of understanding between Libya and Italy enhanced the Italian externalisation policy through the reinforcement of the Libyan Coast Guard's interception and 'pull-back' capacities, through economic, logistic and material support.

In 2018 this externalisation trend intensified. New fund packages and negotiation tables paved the way for future arrangements with third countries to contain migration flows and keep them far away from European borders, under EU blessing and support (European Commission 2019). According to the declaration of the Spanish government, Spain looks at the EU-Turkey model for shaping its further collaboration with Morocco, in order to strengthen Morocco's border controls (Aynaou 2018). Cooperation with Morocco is supported by the European Commission which confirmed that the 'EU has been laying the foundations for a close partnership with Morocco. In late 2018, it approved EUR 140 million in support in border management and budget support,' through the EUTFa (European Commission 2019: 5). The EU also welcomed Italy's cooperation with Libya and in May 2018 it allocated €46 million to support Libyan interdiction capacity (Moreno-Lax & Lemberg-Pederse 2019: 27; European Commission 2018b).

The declared aim of externalisation policies is to ease the burden on coastal states, allowing for more controlled access to Europe while reducing migrants' incentives to undertake dangerous travel. In this sense important results have been achieved, with an overall reduction in irregular border crossings and arrivals in EU. Illegal border crossing has diminished by 95 per cent from its peak in October 2015. The decrease in arrivals corresponded also to a drop in the number of people who died or disappeared while attempting the Mediterranean crossing (in 2018, 28 per cent lower than in 2017) (UNHCR 2019).¹⁰ These results have been presented as a positive impact that externalisation policies have had on migration. Nonetheless, this could be a Pyrrhic victory. While the results on illegal arrivals appear astonishing, they may hide a different reality. The

10 The death rate decreased in absolute terms, but increased in relative terms. See n 8.

containment of migrants within third countries implies a serious compression of their human rights.

In 2018, with Resolution 2228, the Parliamentary Assembly of the Council of Europe (PACE) expressed concerns about externalisation policies because 'the countries concerned may not have equivalent human rights standards or legal instances to uphold them, whereas asylum seekers face difficulties in holding the European Union or individual states responsible for possible human rights violations'. (PACE 2018: para 6).

In fact, the EU-Turkey statement has raised widespread criticism. The PACE questioned Turkey's capacity to ensure adequate protection, effective access to asylum procedures and remedies against return decisions, and defined the return to Turkey of non-Syrian refugees as contrary to EU and international law (PACE 2016). Several NGOs and international organisations denounced that, following the agreement, the new political collaboration between Greece and Turkey resulted in systematic 'push-backs' from Greece to Turkey and illegitimate detentions (ECRE 2017b; HRW 2018). In 2018 the European Committee for the Prevention of Torture affirmed that '[t]he delegation received several consistent and credible allegations of informal forcible removals (push-backs) of foreign nationals by boat from Greece to Turkey at the Evros River border by masked Greek police and border guards or (para-)military commandos' (CPT 2018: 6).

Similarly, 'push-back' practices have been widely documented at the border between Spain and Morocco. In 2017 the European Court condemned Spain for illegal 'push-backs' (*ND & NT v Spain* 2017: para 122). Moreover, several NGOs raised concerns about authorities taking repressive measures to stop people from reaching Spain (ECRE 2019a).

European cooperation with Libya has also been widely criticised since the possibility to consider Libya a 'safe third country' faltered. In April 2018 the Office of the United Nations Commissioner for Human Rights denounced the inhuman conditions of Libyan detention centres for refugees (OHCHR 2018a). Conditions were confirmed by reports of the United Nations Support Mission in Libya and several NGOs. Apparently, the containment of migrants in third countries comes at the expense of human rights.

3.3 Shifting responsibilities

The principal effects and, arguably, aim of externalisation policies are getting responsibility away from EU member states, while maintaining control over migration management. In other words, member states carry out migration control by proxy (Moreno-Lax & Giuffré 2019: 85). Yet, in *Hirsi & Others v Italy* (2012) and, more recently, in *ND & NT v Spain* (2017), the European Court opened a breach in the scheme of externalisation of responsibility, ruling that states are accountable every time they exercise *de facto* control over migrants, even extraterritorially, regardless of political agreements they may have concluded with other states.

As a consequence, states are adjusting their practice accordingly. Enhancing third countries' border control and pull-back practices is aimed at preventing any contact with migrants that could lead to their

accountability. This is an interesting reading when looking at the multiple EU and Italian efforts to support the Libyan Coast Guard operationally. The European Council's remark whereby 'all vessels operating in the Mediterranean must ... not obstruct operations of the Libyan Coastguard' is remarkable (European Council 2018: 1). Arguably, this aims at preventing the intervention of EU member states-flagged vessels from being an obstacle to contactless control over migration, especially when these vessels carry rescued persons to Europe (Maiani 2018). This could add a new perspective to the proposal of regional disembarkation platforms, which encourages EU member states-flagged vessels to disembark rescued people in third countries.

Moreover, consistent with the attempts to avoid any contact with migrants, the EU Parliament recently voted against a resolution on search and rescue in the Mediterranean which called on states 'to enhance proactive search and rescue operations by providing sufficient vessels equipment ... and personnel; ... to make use of all vessels able to assist [search and rescue operations] including NGOs; ... to maintain their ports open to NGOs' (EP 2019).

However, international law has some guarantees to prevent states from outsourcing their responsibility (Goodwin-Gill 2007: 34). As posited by Moreno-Lax and Giuffr , the wide support and the weight of the reciprocal commitments in place (involving economic, technical, logistical and political aspects) could lead to ground the state responsibility at least on articles 16 and 17 of the International Law Commission Draft Articles on State Responsibility (DASR), respectively, 'aid or assistance in the commission of an internationally wrongful act' and 'direction and control exercised over the commission of an internationally wrongful act' (Moreno-Lax & Giuffr  2019: 100-108).

The EU Fundamental Rights Agency itself affirmed that 'state responsibility may exceptionally arise when a state aids, assists, directs and controls or coerces another state to engage in conduct that violates international obligations' (FRA 2016: 2). Moreover, Moreno-Lax and Giuffr  pointed out that under the European Convention states have obligations not to engage in actions that imperil human rights, including the prohibition for a state to enter into agreements with other states that conflict with its obligations under the Convention (Moreno-Lax & Giuffr  2019: 105). Thus, the eventual violation by the third country 'will be jointly attributable to the [third country] and the EU MS for their independent contribution to a single harmful outcome', in line with article 47 of DASR (Moreno-Lax & Giuffr  2019: 105).

An important decision against the externalisation of responsibilities could be provided by the European Court. As mentioned, in the landmark *Hirsi* judgment the Court extended the edges of states' accountability. With its decision in *ND & NT v Spain* it appears to be willing to take a strong stance on migration control (Pijnenburg 2018: 407). The Court now has a new opportunity to lead the way for a more extensive interpretation of state responsibility. In the aforementioned *GLAN-ASGI* case, brought before the Court in May 2018, Italy allegedly was responsible for a Libyan Coast Guard operation that occurred in November 2017, involving several human rights violations. Loredana Leo, a chief lawyer of ASGI, stated that '[f]or the first time, the question of the direct responsibility of the Italian state in the Libyan Coast Guard

interventions and in the *refoulement* carried out in Libya by the latter is raised before the ECtHR' (ECRE 2018b). If the Court should rule against Italy, and depending on the legal reasoning it adopts, a historical chapter on state responsibility could be written, with great potential to have an impact on externalisation policies altogether and to further the effectiveness of human rights protection.

Another factor worth considering is whether the EU itself could be held responsible for its key role in the development and implementation of externalisation policies. In this case, a new chapter could be opened for the Court of Justice of the European Union (CJUE), which would be called upon to decide on EU responsibility for its migration control policy. In the three cases *NF, NG and NM v European Council* (2017) the Court affirmed its lack of jurisdiction over the EU-Turkey deal, holding that the deal was attributable to the Heads of State and Government of the member states and not to the EU itself. However, the involvement and proactivity of the EU in pursuing and supporting externalisation arrangements with third countries could lead to different outcomes in the future.

Importantly, under the Rome Statute the International Criminal Court (ICC) has jurisdiction over states' practices that engage (even indirectly) in internationally wrongful acts and grave human rights violations. Based on this consideration, a group of academics in March 2018 called on the ICC Prosecutor to open *motu proprio* an investigation on the role of Italian authorities into crimes against humanity committed in Libya.¹¹ While the ICC has since 2011 been investigating crimes against humanity and war crimes committed in Libya, including against migrants, it has been pointed out that the complicity of European actors should also be part of the investigation, under penalty of the Court's being accused of bias and conducting selective prosecution (Mann 2018).

A team of international lawyers recently submitted a communication to the Office of the Prosecutor of the ICC concerning 'EU migration policies in the Central Mediterranean and Libya', arguing that the EU and its member states enacted a 'premeditated and intentional practice of non-assistance of migrant boats in distress at sea' (Branco 2019: para 32). It is further argued that the EU's 'externalisation of maritime and human rights obligations' constitutes 'a (failed) attempt to avoid exposure to these legal responsibilities' (Branco 2019: para 450). Notwithstanding the difficult challenge of identifying the high-level officials responsible for the alleged crimes, this communication is a good opportunity for the ICC to not only enhance its credibility and wash away the accusation of being biased, but also to end the impunity of Western actors for international crimes and further the effective protection of human rights.

3.4 Concluding remarks

As observed throughout the article, the recent developments regarding European asylum and migration policies show the intrinsic tension between the aspirations of unity and harmonisation of the EU's foreign policy and the claims of sovereignty by the member states, reluctant to cede control over their national borders.

11 See the statement by 29 academics on Italy seizing the rescue boat Open Arms, <http://statewatch.org/news/2018/mar/open-arms-statement.pdf>.

The inability of EU institutions to respond to the needs of countries with greater migratory pressure has resulted in the search for inter-governmental solutions such as *ad hoc* bilateral and multilateral agreements (both within and beyond the EU) that not only fall outside the EU asylum *acquis*, but some of them even raise questions about its compliance with EU law (EDA 2018).

However, one must avoid misunderstandings: The EU and its member states seem to have the same priority, namely, to discourage migrants from entering the EU by keeping migration flows far away from European borders and, in so doing, avoiding legal responsibility. This is clearly reflected in the confirmation *en bloc* of the externalisation measures so far taken by the European Council, which used the June 2018 meeting – and those following – to introduce new elements to the ‘externalisation toolkit’ instead of pushing for a comprehensive CEAS reform, thus avoiding ‘a divisive debate on internal solidarity’ (Maiani 2018).

Nonetheless, important changes can arise after the May 2019 European Parliament elections. Under the ‘unfinished business rule’, the new Parliament will decide whether to revive the CEAS reform and whether to keep it as a package or as individual proposals. Unfortunately, since ‘strengthening external controls’ and ‘enhancing return policies’ are the key messages of the 2019-2024 European Council Agenda (Bamberg 2019), it is difficult to be optimistic about a change in the policy trend.

4 Conclusion

Migration and asylum certainly represented one of the major issues affecting Europe throughout 2018. The international process leading to the Global Compact, considered a milestone for the protection of refugees and migrants, introduced two issues of great relevance: the need for the international community to urgently address the link between climate change and migration; and the need to overcome the traditional distinction between refugees and migrants acknowledging that they are similarly vulnerable and that both categories are entitled to protection under international human rights law. These issues have been particularly controversial during the Global Compact negotiations, generating tensions within the EU and between member states and EU institutions.

These tensions are also clearly reflected in the selected developments within the field of EU migration and asylum policies. The inability of EU institutions to solve the main obstacles preventing the establishment of a truly common EU approach based on equal solidarity and the member states’ unwillingness to cede control over their national borders led to the adoption and implementation of externalisation policies aimed at avoiding legal responsibility for migrants at both the national and supranational levels.

In short, there is a clear gap between the legal and political spheres, and between international and national aspirations. At the universal level there is a legal trend towards a human rights-based approach to migration aimed at ensuring the effective protection of the human rights of all migrants regardless of their legal status. On the other hand, at the national (and European) level there is a political trend to address migration through an

increasingly securitarian and border-control approach, leading to a dramatic limitation of international protection.

Despite the general trend of closure towards migration, it appears that judicial institutions at national, EU and especially regional level (European Court) could play an important role in limiting attempts by the EU and member states to outsource their responsibilities, thus ensuring more effective human rights protection. Yet, judicial decisions cannot be the answer to complex political issues. Only a political process leading to a structural change in the approach to migration can provide a truly sustainable solution. The Global Compact may be a positive step in this direction.

References

- Atak I, Nakache D, Guild E & Crépeau F “Migrants in vulnerable situations” and the Global Compact for Safe Orderly and Regular Migration’ (2018) 273 *Legal Studies Research Paper* 1
- Ayanou R ‘The Spanish-Moroccan border: Forgotten refugee zone’ (2018) *RefLaw*, available at <http://www.reflaw.org/the-spanish-moroccan-border-forgotten-refugee-zone/> (last visited 16 October 2019)
- Bamberg K, Neidhardt A, Brouwershaven I & De Somer M ‘Policy Update July 2019’ (2019) *European Programme for Integration and Migration*, available at <https://www.epim.info/wp-content/uploads/2019/07/EPIM-Policy-Update-July-2019.pdf> (last visited 27 October 2019)
- Basaran T ‘Saving lives at sea: Security, law and adverse effects’ (2014) 16 *European Journal of Migration and Law* 365
- Behrman S & Kent A ‘Overcoming the legal impasse? Setting the scene’ in S Behrman & A Kent (eds) *Climate refugees: Beyond the legal impasse?* (2018) London and New York: Routledge 3-15
- Boffey D ‘African Union seeks to kill EU plan to process migrants in Africa’ *The Guardian* 24 February 2019, available at <https://www.theguardian.com/world/2019/feb/24/african-union-seeks-to-kill-eu-plan-to-process-migrants-in-africa> (last visited 20 October 2019)
- Branco J & Shatz O ‘EU migration policies in the Central Mediterranean and Libya (2014-2019)’ Communication to the Office of the Prosecutor of the International Criminal Court Pursuant to Article 15 of the Rome Statute, available at <http://www.statewatch.org/news/2019/jun/eu-icc-case-EU-Migration-Policies.pdf> (last visited 30 October 2019)
- Carrera S & Cortinovis R ‘The Malta declaration on search and rescue and relocation: A predictable EU solidarity mechanism?’ (2019a) *CEPS Policy Insights*, available at https://www.ceps.eu/wp-content/uploads/2019/10/PI_2019_14_SCRC_Malta-Declaration-1.pdf (last visited 24 October 2019)
- Carrera S & Cortinovis R ‘Search and rescue, disembarkation and relocation arrangements in the Mediterranean. Sailing away from responsibility?’ (2019b) *CEPS Papers in Liberty and Security in Europe*, available at https://www.ceps.eu/wp-content/uploads/2019/06/LSE2019-10_ReSoma_Sailing-Away-from-Responsibility.pdf (last visited 26 October 2019)

- Carrera S, Lannoo K, Stefan M & Vosyliūtė L 'Some EU governments leaving the UN Global Compact on Migration: A contradiction in terms?' (2018) 15 *CEPS* 1
- CJUE *Council of the European Union v Commission* (2016) C-660/13
- CJUE *NF v European Council* (2017) T-192/16
- CJUE *NG v European Council* (2017) T-193/16
- CJUE *NM v European Council* (2017) T-257/16
- Comitato parlamentare di controllo sull'attuazione dell'Accordo di Schengen, di vigilanza sull'attività di Europol, di controllo e vigilanza in materia di immigrazione, 'Resoconto stenografico. Seduta n 41', 22 March 2017, available at http://documenti.camera.it/leg17/resoconti/commissioni/stenografici/html/30/indag/c30_confini/2017/03/22/indice_stenografico.0041.html (last visited 20 October 2019)
- Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE) *Report A5-0315/2000* of 25 October 2000, available at <https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2000-0315+0+DOC+PDF+V0/EN> (last visited 14 October 2019)
- Council of the EU 'Guidelines on Temporary Arrangements for Disembarkation' 12 June 2019 [WK 7219/2019 INIT], available at <https://www.statewatch.org/news/2019/jun/eu-council-wk-guidelines-on-temporary-arrangement-disembarkation.pdf>, (last visited 29 October 2019)
- Cuddy A 'La Libia crea la sua zona search and rescue e notifica l'IMO (con il sostegno UE)' *Euronews* 9 July 2018, available at <https://it.euronews.com/2018/07/09/la-libia-crea-la-sua-zona-sar-e-notifica-l-imo-con-il-sostegno-ue/> (last visited 29 October 2019)
- Cuttitta P 'Repoliticisation through search and rescue? Humanitarian NGOs and migration management in the Central Mediterranean' (2018) 23 *Geopolitics* 632
- Danish Refugee Council 'Rights at risk: Implications of a closer nexus between asylum and return procedures' DRC Policy Brief *DRC News* 30 April 2019, available at <https://drc.ngo/news/rights-at-risk-implications-of-a-closer-nexus-between-asylum-and-return-procedures> (last visited 29 October 2019)
- Decreto-Legge 14 giugno 2019 n. 53, convertito con modificazioni in Legge 8 agosto 2019 n. 77, GU 09/08/2019, n. 186)
- ECRE 'Asylum at the European Council 2018: Outsourcing or reform?' (2018a) ECRE Policy Papers, available at <https://www.ecre.org/wp-content/uploads/2018/08/Policy-Papers-04.pdf> (last visited 29 October 2019)
- ECRE 'Case against Italy before the European Court of Human Rights will raise issue of cooperation with Libyan Coast Guard' (2018b) *ECRE News* 18 May 2018, available at <https://www.ecre.org/case-against-italy-before-the-european-court-of-human-rights-will-raise-issue-of-cooperation-with-libyan-coast-guard/> (last visited 15 October 2019)
- ECRE 'Debunking the "safe third country" myth' (2017a) Policy note #8, available at <https://www.ecre.org/wp-content/uploads/2017/11/Policy-Note-08.pdf> (last visited 10 October 2019)
- ECRE 'EU report links drop in arrivals to Spanish Moroccan cooperation' (2019a) *ECRE News* 3 May 2019, available at <https://www.ecre.org/eu-report-links-drop-in-arrivals-to-spanish-moroccan-cooperation/> (last visited 23 October 2019)
- ECRE 'Greece: Court curtails detention in the context of the EU-Turkey deal' (2017b) *ECRE News*, 10 November 2017, available at <https://www.ecre.org/greece-court-curtails-detention-in-the-context-of-the-eu-turkey-deal/> (last visited 22 October 2019)

- ECRE 'Operation "Sophia" is given six more months without ships' (2019b) *ECRE News*, 29 March 2019, available at <https://www.ecre.org/operation-sophia-is-given-six-more-months-without-ships/> (last visited 29 October 2019)
- ECRE 'The implementation of the hotspots approach in Italy and Greece: A study' (2016) *ECRE Reports*, available at <https://www.ecre.org/wp-content/uploads/2016/12/HOTSPOTS-Report-5.12.2016..pdf> (last visited 29 October 2019)
- ECtHR *ND & NT v Spain* (2017)
- EU Fundamental Rights Agency (FRA) 'Guidance on how to reduce the risk of *refoulement* in external border management when working in or together with third countries' (2016) *EU Publications*, available at <https://fra.europa.eu/en/publication/2016/guidance-how-reduce-risk-refoulement-external-border-management-when-working-or> (last visited 24 October 2019)
- EU Fundamental Rights Agency (FRA) '2019 update – NGO ships involved in search and rescue in the Mediterranean and criminal investigations' (2019) *FRA online publications*, available at <https://fra.europa.eu/en/publication/2019/2019-update-ngos-sar-activities> (last visited 18 October 2019)
- EU Statement on international cooperation during the 4th round of negotiation of the Global Compact on Migration of 15 May 2018, available at https://refugees.migrants.un.org/sites/default/files/eu_proposal_on_international_cooperation.pdf (last visited 13 October 2019)
- European Commission 'EU trust fund for Africa: Additional €90.5 million to strengthen border management and protection of migrants in North Africa' (2018a) *European Commission News*, 6 July 2018, available at https://ec.europa.eu/trustfundforafrica/all-news-and-stories/eu-trust-fund-africa-additional-eu905-million-strengthen-border-management-and_en (last visited 17 October 2019)
- European Commission 'EU cooperation on migration in Libya' (2018b) *Facsheet*, available at <https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/euf-noa-ly-08052018.pdf> (last visited 28 October 2019)
- European Commission 'Progress report on the Implementation of the European Agenda on Migration' COM (2019) 126 final
- European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) Preliminary observations on the visit of Greece [CPT/Inf (2018) 20] (2018)
- European Consensus on Development 'Our world, our dignity, our future' (2017), available at https://ec.europa.eu/europeaid/sites/devco/files/european-consensus-on-development-final-20170626_en.pdf (last visited 14 October 2019)
- European Council 'EU-Turkey statement' (2016a) *Press release*, 18 March 2016, available at <https://www.consilium.europa.eu/en/press/press-releases/2016/03/18/eu-turkey-statement/> (last visited 17 October 2019)
- European Council Conclusions 21 October 2016 [EUCO 31/16] (2016b)
- European Council Conclusions 28 June 2018 [EUCO 9/18] (2018)
- European Database of Asylum Law (EDA) 'The case of the administrative arrangement between Greece and Germany: A tale of "paraDublin activity"?' *EDA Journal* 5 November 2018, available at <https://www.asylumlawdatabase.eu/en/journal/case-administrative-arrangement-between-greece-and-germany-tale-%E2%80%9Cparadublin-activity%E2%80%9D> (last visited 27 October 2019)
- European Parliament Resolution on progress on the UN Global Compacts for Safe, Orderly and Regular Migration and on Refugees [2018/2642(RSP)] (2018)
- European Parliament Resolution on the situation in the Mediterranean and the need for a holistic EU approach to migration [2014/2907(RSP)] (2014)

- European Parliament Motion for a Resolution on search and Rescue in the Mediterranean [2019/2755(RSP)] (2019)
- Felipe Pérez B 'Beyond the shortcomings of international law' in Behrman S et al (eds) *Climate refugees: Beyond the legal impasse?* (2018) London and New York: Routledge 214
- Fernandez RF & Rubio J 'Boat caught in Europe's migration spat brings hundreds to Spain' (2018) *Reuters*, available at <https://www.reuters.com/article/us-europe-migrants-italy-spain/migrant-boat-turned-away-by-italy-arrives-in-spain-idUSKBN1JD033> (last visited 20 October 2019)
- Financial Times* 'EU border force accuses charities of collusion with migrant smugglers' *Financial Times* 15 December 2016, available at <https://www.ft.com/content/3e6b6450-c1f7-11e6-9bca-2b93a6856354> (last visited 20 October 2019)
- Fine S 'All at sea: Europe's crisis of solidarity on migration' (2019) European Council on Foreign Relations, available at https://www.ecfr.eu/page/-/all_at_sea_europes_crisis_of_solidarity_on_migration.pdf (last visited 25 October 2019)
- Frelick B, Keyser MI & Podkul J 'The impact of externalisation of migration controls on the rights of asylum seekers and other migrants' (2016) 4 *Journal on Migration and Human Security* 190
- Frontex 'Frontex launching new operation in Central Med' (2018) *Frontex News*, 1 February 2018, available at <https://frontex.europa.eu/media-centre/news-release/frontex-launching-new-operation-in-central-med-yKqSc7> (last visited 29 October 2019)
- Gammeltoft-Hansen T et al 'What is a compact? Migrants' rights and state responsibilities regarding the design of the UN Global Compact for Safe, Orderly and Regular Migration' (2017) Raul Wallenberg Institute
- Gatti M 'EU states' exit from the Global Compact on Migration: A breach of loyalty' (2018) EU Immigration and Asylum Law and Policy, available at <http://eumigrationlawblog.eu/eu-states-exit-from-the-global-compact-on-migration-a-breach-of-loyalty/> (last visited 22 October 2019)
- Global Legal Action Network 'Case filed against Greece in Strasbourg court over crackdown on humanitarian organisations' *GLAN News* 18 April 2019, available at <https://www.glanlaw.org/single-post/2019/04/18/Case-filed-against-Greece-in-Strasbourg-Court-over-Crackdown-on-Humanitarian-Organisations> (last visited 25 October 2019)
- Global Legal Action Network 'Legal action against Italy over its coordination of Libyan Coast Guard pull-backs resulting in migrant deaths and abuse' *GLA News* 8 May 2018, available at <https://www.glanlaw.org/single-post/2018/05/08/Legal-action-against-Italy-over-its-coordination-of-Libyan-Coast-Guard-pull-backs-resulting-in-migrant-deaths-and-abuse> (last visited 29 October 2019)
- Goodwin-Gill G 'The extraterritorial processing of claims to asylum or protection: The legal responsibilities of states and international organisations' (2007) 9 *UTS Law Review* 26
- Guild E 'The UN Global Compact for Safe, Orderly and Regular Migration: What place for human rights?' (2018) 30 *International Journal of Refugee Law* 661
- Guild E & Grant S 'What role for the EU in the UN negotiations on a Global Compact on Migration?' (2017) 5 *CEPS* 1
- Human Rights Watch (HRW) 'Greece: Violent pushbacks at Turkey border' *HRW News* 18 December 2018, available at <https://www.hrw.org/news/2018/12/18/greece-violent-pushbacks-turkey-border> (last visited 22 October 2019)
- IOM 'Global Compact on Migration' (2018), available at <https://www.iom.int/global-compact-migration> (last visited 22 October 2019)

- Ionesco D 'Let's talk about climate migrants, not climate refugees – Think piece on the sustainable development knowledge platform' *UN Blog* 6 June 2019, available at <https://www.un.org/sustainabledevelopment/blog/2019/06/lets-talk-about-climate-migrants-not-climate-refugees/> (last visited 22 October 2019)
- Italian Parliamentary Question presented in 2018 (Assemblea 3-00337), available at <https://aic.camera.it/aic/scheda.html?numero=3-00337&ramo=C&leg=18> (last visited 22 October 2019)
- Kälin W 'The Global Compact on Migration: A ray of hope for disaster-displaced persons' (2018) 30 *International Journal of Refugee Law* 664
- Maiani F "'Regional disembarkation platforms" and "controlled centres": Lifting the drawbridge, reaching out across The Mediterranean, or going nowhere?' (2018) *Reflaw*, available at http://www.reflaw.org/regional-disembarkation-platforms-and-controlled-centres-lifting-the-drawbridge-reaching-out-across-the-mediterranean-or-going-nowhere/#_ednref3 (last visited 26 October 2019)
- Mann I, Moreno-Lax V & Shatz O 'Time to investigate European Agents for Crimes against Migrants in Libya' *European Journal of International Law Blog* 29 March 2018, available at <https://www.ejiltalk.org/time-to-investigate-european-agents-for-crimes-against-migrants-in-libya/> (last visited 30 October 2019)
- McAdam J 'The Global Compacts on Refugees and Migration: A new era for international protection?' (2019) 30 *International Journal of Refugee Law* 571
- Melin P 'The Global Compact for Migration: Lessons for the unity of EU representation' (2019) 21 *European Journal of Migration and Law* 194
- Ministero dell'Interno 'Codice di Condotta per le ONG impregnate in attività di ricerca e soccorso in mare', available at https://www.interno.gov.it/sites/default/files/codice_condotta_ong.pdf (last visited 20 October 2019)
- Ministero dell'Interno 'Direttiva N 14100/141(8)' 15 April 2019, available at https://www.interno.gov.it/sites/default/files/direttiva_del_ministro_n._14100_1418_15_aprile_2019.pdf (last visited 18 October 2019)
- Moreno-Lax V & Giuffré M 'The rise of consensual containment: From "contactless control" to "contactless responsibility" for forced migration flows' in S Juss (ed) *Research handbook on international refugee law* (2019) Edward Elgar Publishing 82
- Moreno-Lax V & Lemberg-Pederse M 'Border-induced displacement: The ethical and legal implications of distance-creation through externalisation' (2019) 56 *QIL, Zoom-in* 5
- Neidhardt A et al 'Policy update October 2019' (2019) European Programme for Integration and Migration, available at <https://www.epim.info/wp-content/uploads/2019/10/October-2019.pdf> (last visited 27 October 2019)
- Nicolosi S 'Reforming the common European asylum system: Business as usual?' (2019) *Reflaw*, available at <http://www.reflaw.org/reforming-the-common-european-asylum-system-business-as-usual/> (last visited 27 October 2019)
- Parliamentary Assembly of the Council of Europe (PACE) Resolution 2109 (2016) of 20 April 2016
- Parliamentary Assembly of the Council of Europe (PACE) Resolution 2228 (2018) of 27 June 2018
- Pastore F 'Not so global, not so compact. Reflections on the shitstorm surrounding the Global Compact for Migration' (2019) 19 *IAI Commentaries* 1
- Pijnenburg A 'From Italian pushbacks to Libyan pullbacks: Is Hirsi 2.0 in the making in Strasbourg?' (2018) 20 *European Journal of Migration and Law* 296

- Pilkey O 'The cruelest wave: Climate refugees' in O Pilkey, L Pilkey-Jarvis & K Pilkey *Retreat from a rising sea: Hard choices in an age of climate change* (2016) Columbia University Press 127
- Piper N 'The Global Compact on Migration' (2018) 18 *Global Social Policy Forum* 323
- Pollet K 'All in vain? The fate of EP positions on asylum reform after the European elections' (2019) EU Immigration and Asylum Law and Policy, available at <http://eumigrationlawblog.eu/all-in-vain-the-faith-of-ep-positions-on-asylum-reform-after-the-european-elections/> (last visited 26 October 2019)
- SOS Méditerranée 'On instructions from Rome, the Aquarius is stopped at sea between Malta and Italy, waiting for a safe port to disembark 629 survivors' Press Release 11 June 2018, available at <https://sosmediterranee.com/press/on-instructions-from-rome-the-aquarius-is-stopped-at-sea-between-malta-and-italy-waiting-for-a-safe-port-to-disembark-629-survivors/> (last visited 20 October 2019)
- Sundenberg Diez O, Bamerd K, De Somer M & McNamara F 'Policy update December 2018' (2018) EPIM, available at <https://www.epim.info/wp-content/uploads/2018/12/December-2018-EPIM-Policy-Update.pdf> (last visited 22 October 2019)
- Trevisanut S 'Search and rescue operations in the Mediterranean: Factor of cooperation or conflict?' (2010) 25 *The International Journal of Marine and Coastal Law* 523
- Tsirogianni C 'Common European asylum system reform. Main issues and challenges' (2018) *Jean Monnet European Centre of Excellence*, available at <https://jmce.gr/portal/wp-content/uploads/2018/08/Tsirogianni-COMMON-EUROPEAN-ASYLUM-SYSTEM-REFORM.pdf> (last visited 27 October 2019)
- UN Communication Office 'U-turns on Global Compact "reflect poorly" on countries concerned: Senior UN migration official' *UN News* 27 November 2018, available at <https://news.un.org/en/story/2018/11/1026791> (last visited 22 October 2019)
- UN General Assembly (UNGA) Resolution on Modalities for the intergovernmental negotiations of the global compact for safe, orderly and regular migration [A/RES/71/280] (2017)
- UN General Assembly (UNGA) Resolution on the Adoption of the New York Declaration for Refugees and Migrants [A/RES/71/1] (2016a)
- UN General Assembly (UNGA) Resolution on the Global Compact for Safe, Orderly and Regular Migration [A/RES/73/195] (2018)
- UN General Assembly (UNGA) Resolution on Human rights defenders in the context of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms [A/RES/70/161] (2016b)
- UN Refugee Agency (UNHCR) 'Migrants in vulnerable situations': UNHCR's perspective' (2017), available at <https://www.refworld.org/pd/596787174.pdf> (last visited 22 October 2019)
- UN Refugee Agency (UNHCR) Operational portal refugee status (2019), available at <https://data2.unhcr.org/en/situations/mediterranean> (last visited 22 October 2019)
- UN Regional Consultations on the Compact for Migration, available at <https://refugeesmigrants.un.org/regional-consultations> (last visited 22 October 2019)
- United Nations Human Rights Office of the High Commissioner (OHCHR) 'Joint Communication from Special Procedures' [AL/ITA/4/2019] (2019), available at

<http://www.statewatch.org/news/2019/may/un-it-sr-letter-directive-sar-libya-human-rights-5-19.pdf> (last visited 25 October 2019)

United Nations Human Rights Office of the High Commissioner (OHCHR) 'Abuse behind bars: Arbitrary and unlawful detention in Libya' (2018a), available at https://www.ohchr.org/Documents/Countries/LY/AbuseBehindBarsArbitraryUnlawful_EN.pdf (last visited 9 October 2019)

United Nations Human Rights Office of the High Commissioner (OHCHR) 'Comments on the reform of the European migration and asylum system' [OL OTH 64/2018] (2018b), available at https://www.ohchr.org/Documents/Issues/SRMigrants/Comments/OL_OTH_64_2018.pdf (last visited 1 October 2019)

United Nations Human Rights Office of the High Commissioner (OHCHR) and United Nations Support Mission in Libya (UNSMIL) 'Desperate and dangerous: Report on the human rights situation of migrants and refugees in Libya' (2018), available at <https://www.ohchr.org/Documents/Countries/LY/LibyaMigrationReport.pdf>, (last visited 29 October 2019)

Selected developments in human rights and democratisation during 2018: Could it have been worse? Mixed messages around democracy and human rights in the Asia Pacific

Ravi Prakash Vyas,* Mike Hayes, Nanang Indra Kurniawan*** and Longgina Novadona Bayo******

Abstract: During 2018 the downward slide in human rights and democracy across the Asia Pacific region was slowed down, but not reversed. Many of the concerns gripping the region, such as the treatment of the Rohingya by the Myanmar state, the violence of the Duterte regime in the Philippines, and China's cavalier attitude towards rights, remained shocking but did not worsen. In a few areas human rights or democracy improved. One shining light is the Malaysian election where the heavily corrupt governing party, which had been in power since Malaysia's independence, was voted out. Even though the party controlled the media, manipulated the electoral system, and used a campaign of misinformation during the election, Malaysians bravely voted for a more democratic future. Across the region concerns have been raised about China's increasing economic, political and military influence, but at the same time others have praised the development it has enabled. Global trends, such as the #metoo movement, the global conference on climate change, and the Global Migration Compact have had an impact on the region, but not enough to declare the region to be positively embracing these developments. All these factors show that there is a mixed response to human rights and democracy: The existence of serious violations and disturbing trends means that the region remains in an epoch where authoritarianism holds sway. The actions of these governments are open to condemnation by civil society and the possibility of a change in opinion about these actions. However, there is little evidence that this will happen in the near future.

Key words: human rights; democratisation; Asia Pacific; Rohingya; Duterte regime; human rights in China; authoritarianism

* BA LLB (Hons) (GGSIU, India) MHRD (The University of Sydney, Australia); Assistant Professor of International Law and Human Rights, Kathmandu School of Law, Nepal; Project Coordinator of the APMA Programme under the Global Campus of Human Rights; rpvyas@ksl.edu.np

** PhD (Wollongong University); Programme Director of the APMA programme; Lecturer, Institute of Human Rights and Peace Studies, Mahidol University.

*** PhD (Melbourne University); Lecturer, Department of Politics and Government Sciences, Universitas Gadjah Mada.

**** MA (Universitas Gadjah Mada); Lecturer, Department of Politics and Government Sciences, Universitas Gadjah Mada, novabayo@ugm.ac.id

1 Key issues

1.1 The Rohingya crisis

For the past four years the Rohingya crisis has continued to constitute one of the most significant systematic human rights violations in the region. Historically, there has been tension between the Myanmar state and the Rohingya minority living in Rakhine state in Western Myanmar, which is one of hundreds of ethnic, minority and indigenous groups in Myanmar. The Rohingyas have always lived in this area, although they share ethnic and religious similarities with neighbouring Bangladesh, and there has been a history of migration between Bangladesh and Rakhine state. Rohingyas face discrimination and threats of expulsion primarily from Buddhist Nationalists because of being Muslim. The military also has targeted this minority as a way of empowering the programme of 'Burmanisation', a policy to ensure that Myanmar's Buddhist, Bamar¹ majority maintains dominance (Burlie 2008).

Since the campaign of ethnic cleansing started in 2017, more than 730 000 Rohingya have been forced across the border to Bangladesh, escaping persecutions, killings, enforced disappearances, sexual violence and starvation. According to Human Rights Watch (2018a), the government did not allow independent investigators to access the conflict area and also punished local journalists for reporting on military abuses. Amnesty International (2018a) also stated that evidence demonstrates that the violence in Myanmar forms part of a well-planned, systematic attack by state forces. For most people fleeing ethnic cleansing Bangladesh is the destination, with over one million refugees currently in the country, although some move on, with populations of Rohingya in Malaysia, Saudi Arabia and Indonesia. While the exodus of Rohingya has slowed down from its peak in 2017, Rohingya in the Rakhine state continue to flee. Many find the conditions of their internment camps in Myanmar unliveable. The camps, apparently constructed to ensure the safety of the Rohingyas, do not provide basic living conditions.

The United Nations (UN) initiated a three-person² fact-finding mission on Myanmar in March 2017. Their report, released in September 2018, called for the prosecution of five leading military figures, calling their actions 'ethnic cleansing' occurring with 'genocide intent'.³ The report detailed war crimes, crimes against humanity and systematic rape. With support from the UN Secretary-General, Antonio Guterres,⁴ the UN Human Rights Council formed the UN Independent International Fact-Finding Mission on Myanmar to investigate violations and collect evidence resulting from the findings of the first mission. Throughout this process the Myanmar government has denied all accusations, claiming that the

1 Bamar (sometimes spelt Burman) are the largest ethnicity in Myanmar, making up approximately 68% of the population, and living along the Ayeyarwadi river and in cities such as Yangon and Mandalay.

2 The members were: Marzuki Darusman from Indonesia (who previous sat on bodies investigating Benazir Bhutto's assassination and war crimes in Sri Lanka), Ms. Radhika Coomaraswamy from Sri Lanka (who previously was the special rapporteur for violence against women), and Chris Sidoti from Australia (who was once on the Chair of the Australian Human Rights Commission).

3 See the fact finding report Para 84-87 (Human Rights Council 2018).

4 See in particular Secretary General (2018)

report did not reflect the reality on the ground. Aung San Suu Kyi, once seen as the hero of the democratic movement and a leading figure in the human rights movement, faced criticism from the international community, first for her failure to act, and later for her complicity in the denial of the atrocities. Her name has been removed from various awards and is no longer praised in civil society (Goldberg 2018). Facebook was widely criticised as the platform used to spread hate speech among the Buddhist Nationalists and supporters of the ethnic cleansing. As it is one of the few social media platforms to have Burmese script, it is extremely popular in Myanmar, and for many was their introduction to the internet. However, this group of early internet users had little experience in social media, and may not have had the skills to identify the many false claims made on this platform (Mozur 2018; BBC trending 2008). By the end of 2018 little had been achieved to address the situation. Myanmar claimed that it was willing to take back refugees, and around 2 000 people were reported to have returned, but this number is low given the one million refugees in neighbouring countries. UN investigations continue, but it is unlikely that the Myanmar military generals will face trial, as Security Council members such as China indicated that they do not support an International Criminal Court (ICC) investigation. These questions of accountability of the generals will be addressed in 2019.

1.2 China's influence in the region

China's influence regarding human rights in the region is threefold. China influences the human rights standards in countries it supports either politically or economically; it influences human rights processes at UN bodies by promoting its own views on human rights, and it influences how human rights violations are reported in its own country. These will be discussed in turn. First, China's economic and social development has for some enabled development, expanded economies, and increased opportunities for trade. China has replaced the often-disliked interventionist economic policies of the World Bank and the International Monetary Fund (IMF) with less restrictive access to loans. Furthermore, the large-scale infrastructure plan of the Belt and Road Initiative (BRI) is expected to boost the economy of lesser-developed countries, such as Pakistan, Sri Lanka and Laos PDR. On the other hand, critics are concerned that China's economic influence been accompanied by territorial expansion, particularly its claim over large parts of the South China Sea (which has been rejected by the Tribunal for the Convention of the Law of the Sea). The economic expansion may also influence politics in the region, for example by propping up undemocratic states or creating a 'new form of colonialism' as stated by Malaysian leader Mahathir Mohamed (ABC 2018). For South Asia, it is asked whether Chinese diplomacy on human rights affects the adoption of the internationally-accepted rights in the South Asian countries.

Second, at the UN China has in the past few years been developing its own theory of human rights. This was elaborated at the recent Universal Periodic Review (UPR) review of China in November 2018, where China explained its new 'concept and theoretical system of human rights with Chinese characteristics' which is the title of a section in the State Under Review report to the UPR process (Worden 2018; Sinopsis 2018). This occurs alongside rising concerns about China's practice of interfering in UN human rights activities, to the extent that a Human Rights Watch

report notes that the 'Chinese delegation's actions have been described as marred by bullying, harassment, and interference' (HRW 2018: 43). The Chinese 'characteristics' of human rights are the emphasis given to the right to development over civil and political rights, alongside the emphasis put on 'national characteristics', meaning that the state's interpretation of rights has priority over the universal interpretation. This 'theory' of human rights harks back to the Asian Values debate prominent in the 1990s, where leaders such as Singapore's Lee Quan Yew and Malaysia's Mahathir Mohammed espoused the view that Asian countries should comply with a different set of human rights, where duties to the community outweigh individual freedoms, and rights only come with obedience to authority. These views were widely rejected, particularly after the 1997 economic crisis which showed that the basis of development over rights relied purely on people's willingness to remain quiet while the economy grew; once there was an economic downturn people demanded participation in politics and held their leaders to account – what should have been very un-Asian values. The key elements of Asian Values have returned in China's version of human rights.

Third, China has to defend its human rights record at home with revelations about the Uyghur re-education camps, first by Human Rights Watch in September 2017 (HRW 2017), but later noted in numerous news and diplomatic reports during 2018. The Xinjiang Uighur Autonomous Region (XUAR) has had unrest and seen separatist movements from the Uyghur ethnic minority. As a response the Chinese government has accused Uyghurs of terrorism and being an 'evil cult'. This has resulted in police harassment, torture, arbitrary detention and imprisonment (HRW 2019a). A 'De-Extremification Regulation' has been enacted in the Autonomous Region, prohibiting a wide range of behaviours labelled 'extremist', such as spreading 'extremist thought', denigrating or refusing to watch public radio and television programmes, wearing burkas, having an 'abnormal' beard, resisting national policies, and reading publications containing 'extremist content' (Amnesty International 2018b). While it is difficult to determine the exact size and function of the camps, they are estimated to have between 100 000 and three million detainees, although the BBC reports around one million detainees (BBC 2018; Stewart 2019), and they are for the function of 're-education', especially by using the thoughts of Chinese leaders such as Xi Jinping, swearing allegiance to China, and undergo self-criticism (Jiang 2018). However, people are mostly detained arbitrarily, with males targeted and families separated. China has denied any violations and claims that the camps are used for education to change potential terrorists' views and prepare them for re-entry into the community.

Another area of concern is China's control and use of technology. China continues to block social media sites such as Facebook (and its applications of Instagram and WhatsApp), but promotes the use of its own social media platforms, although there are questions about the privacy on these platforms. China has been widely criticised for its implementation of cybersecurity law which became effective in June 2018, making it obligatory for internet companies operating in China to censor users' content, and collecting a wide range of personal information through the WeChat which is by far the dominant messaging service (Amnesty International 2018b). China's use of data for surveillance over its population, and its export of this technology to other countries raise

concern. Chinese authorities also continue to harass and detain journalists who cover issues of human rights.

1.3 Ethnic and religious extremism

There are a number of hotspots of ethnic and religious extremism across the region. One of the largest is the government response to the Uyghurs in Xingjiang province in China, as noted above. In India, according to the US Commission for International Religious Freedom report, 'in 2018 religious freedom conditions in India continued a downward trend' (USCIRF 2019). The trend may be linked to the rise in Hindu nationalism, or what the report calls 'the growth of exclusionary extremist narratives' (USCIRF 2019). The government has engaged in attacks against religious minorities by directly or indirectly conducting abuses, killings and abductions, often for supposed 'forced conversions'. There have been cow protection mobs attacking Muslim dairy, leather and beef businesses. In neighbouring Bangladesh, armed groups have targeted Shi'a Muslims. Blasphemy laws that carry the death penalty are used against minority groups in Pakistan. In several countries of Southeast Asia the protection of freedom of religion is also characterised by direct and indirect contributions to the violence by the state. Myanmar has the on-going conflict and abuse by security forces of the Rohingya Muslims, and religious minorities in Vietnam face widespread discrimination. Under such conditions, members of religious minorities were vulnerable and subjected to continuous attacks.

Indonesia specifically has witnessed infringements of freedom of religion through three interrelated activities: the tolerance of hate-speech; claims of blasphemy; and the destruction of places of worship. At least 22 people experienced prosecution under the blasphemy law since Widodo took power in 2014 (Pearson 2018). Aside from the case of Ahok – an ethnic Chinese, Christian former governor of Indonesia's capital who is a well-known victim of this law – numerous other cases have emerged. In August 2018 an ethnic Chinese, Buddhist woman, Meliana, was found guilty of blasphemy and was sentenced to 18 months' imprisonment by a North Sumatran court when she complained of the speaker volume of *adhan* (or the Islamic call to prayer) from a nearby mosque being too loud. The case sparked tension between Buddhists and Muslims in the region, triggering a riot that resulted in the burning down of Meliana's house, several *Vihara* (Buddhist monasteries) and Chinese temples. Some national leaders opposed her prosecution, but others who were well-represented by Zainut Tauhid Sa'adi (Deputy Chairperson of the Council of Indonesian *Ulama* in Jakarta) argued that Meliana used sarcastic words with a ridiculous tone which can be regarded as blasphemy towards Islam.

The case of Meliana demonstrates how minor or personal disputes can rapidly escalate due to the politicisation of religion, resulting in a dangerous fault line between minority and majority social groups. The confrontation was energised by (and resulted in) hoax and provocative messages spreading on social media. According to Suryadinata (2018), ethnic-religious friction between Muslims and non-Muslims, also between Chinese and non-Chinese, persists through the long-lasting social and economic gap between the two. While Muslims blamed the non-Muslims for growing wealthier at their expense, the Chinese and other non-Muslims remain unaware of the Muslim's deep-rooted antipathy towards

them. As the tensions persist, there are no initiatives for reliable channels for communication or negotiation between the groups. In December 2018 local communities in Purbayan Village Yogyakarta, where the majority of residents are Muslims, cut off and destroyed the cross-shaped headstone on a Christian grave in a public cemetery, arguing that the religious symbol was not allowed in the village. Claiming community consensus, local people stated that the dead can be buried without any Christian symbol and that that should be done at the edge of the cemetery, insisting that the centre would in the future be for Muslims only. While religious pluralism is acknowledged, it is not substantially embraced by local communities.

According to Human Rights Watch the Widodo government has failed to realise support for human rights into substantive and meaningful policy initiatives to address religious intolerance (HRW 2019b). An earlier Wahid Foundation report from a 2016 survey noted that numerous cases of violations against religious freedoms were also actively carried out by non-state actors (Wahid Foundation 2017). Religious minorities continued to experience intimidation from government-affiliated institutions and also faced various types of threats of violence from Muslim extremist groups, specifically the Islamic Defenders Front (FPI). The Asia-Pacific Centre for the Responsibility to Protect stated that the most compelling risk in Indonesia was the potential of communal violence between religious minorities and the majority Muslim population (APCR2P 2018). However, the government tends to rely on short-term solutions rather than confronting a deeper, on-going low-level sectarian violence that divides Indonesia.

1.4 #metoo in the region

For many countries in the world the #metoo movement led to the fall of celebrities and the increased concern about women's safety from harassment and sexual violence. The response in the Asia Pacific was more muted. China's #metoo movement gained momentum as prominent academics, journalists and activists were accused on social media of sexual misconduct (Repnikova & Zhou 2018). The movement, as most social movements in China, had to proceed with caution; feminist leaders of a similar movement only three years before were detained before being released on bail, all for claiming an end to sexual harassment (Zheng 2017). China is now considering introducing measures to tackle sexual harassment in the workplace through a draft civil code, which is set to be completed by the end of 2020 (Nathani 2018). However, in neighbouring Japan there were far fewer success stories. This is not because women are better protected, as the scandal over entrance to the top medical college shows that sexism is institutionally ingrained in even the most prominent social institutions. The Tokyo Medical University admitted that for over a decade it had manipulated women's scores to prevent them from gaining entrance, which was soon followed by admissions to two other universities. Experts had suspected that this was the case as only about 30 per cent of enrolments were for women, a number that had curiously not changed even though more women were taking the examinations. The excuses given reflect the deeply-ingrained patriarchal attitude of the education officials: Women were more likely to leave to have families, or because women matured earlier it was making the examination unfair for the less biologically-developed males (Haynes 2018). A similar issue is

found in Myanmar, where the entrance score for medical college depends on gender: Women applicants must score higher marks (Soe 2014).

The #metoo movement did have knock-on effects throughout the region with women in South Korea, Thailand, the Philippines and India initiating social movements, although with limited impact. Each of these countries faces a deeply-entrenched male culture of control. This is obvious in the Philippines where the leader, President Rodrigo Duterte, is known for his sexist comments including rape jokes, cat-calling, and supporting violence against women. In Thailand the military junta oversees a government with the lowest participation of female politicians in the Southeast Asian region, and whose leader is known for sexist comments, including his statement that gender equality will lead to social deterioration and that a women's main purpose is giving birth (Coconuts 2016). India has done little to reduce the widespread violence against women, with a Thomson Reuters Foundation 2018 survey ranking it the most dangerous place in the world for women. Apart from women there has been few developments in rights on sexuality and gender identity. By the end of 2018 only Australia and New Zealand recognised same-sex marriage (although Taiwan was to recognise this right in early 2019). The Chinese government continues to disregard lesbian, gay, bisexual, transgender and intersex (LGBTI) rights, as was made evident by its appeal against the decision in April of the court of first instance ruling that the government's refusal to extend work benefits to the same-sex husband of a civil servant was discrimination based on sexual orientation. A later decision by the Court of Appeal, which ruled that the Immigration Department's refusal to grant a dependant visa to a same-sex civil partner of a foreign professional on a work visa was discriminatory, was also upheld (Amnesty International 2018).

1.5 Indigenous rights

Indigenous people in most parts of the world have been facing systemic discrimination and exclusion from economic and political power. This can be seen from complex threats to their survival such as land dispossession, oppression, as well appropriation of collective resources and knowledge (Bengwayan 2003). Even though there are various global efforts to overcome these discriminatory practices, oppression and marginalisation still occur. There is a lack of participation in decision making, and recognition of indigenous rights throughout the region. The United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) and other international laws make available standards for indigenous people in Asia Pacific to demand national governments to recognise their rights to land and respect for their cultures and ways of life. The instruments provide a basis for legal protection for indigenous people and their land from global capitalism (Radcliffe 2019). However, as shown by cases in Asia Pacific, indigenous people struggle to enforce these rights on governments. It has been noted that the instruments often 'fit quite comfortably with – and was perhaps even facilitated by – neoliberal development models' (Engle 2011). In the Asia Pacific this situation is worsening with the expansion of state developmental projects and investments which demand large areas of land. In Indonesia the state has partially recognised indigenous rights to land, but only in a commercial sense with the establishment of tenured security to induce higher investments by connecting and integrating various extra-legal (or

informal) property systems with a formal legal property system. Between 2016 and 2018 Indonesia's central government handed over customary forests to 18 indigenous communities, and then launched the Complete Systematic Land Registration Programme, to formally register all land in Indonesia by 2025. Yet, the concern is that instead of protecting indigenous land, the formal registration opens this land up to be bought and sold, which may lead to indigenous lands being disposed from its indigenous owners.

In other parts of Asia indigenous people are threatened by the state seeking to expand direct control over land. In September 2018 an amendment to the Vacant, Fallow and Virgin (VFV) Lands Management Law was passed in Myanmar. According to this amendment, all people on VFV land have to apply for a permit by March 2019. Approximately one-thirds of land in Myanmar is regarded by the state as being vacant, fallow or virgin land, with most of this land being located in ethnic states. Civil society organisations in Myanmar see this law as problematic as it ignores the fact that many indigenous people have been using these 'vacant' lands under their traditional laws.

A 2018 report by UN Special Rapporteur on the Rights of Indigenous Peoples shows the increased use of physical violence and criminalisation against indigenous peoples (OHCHR 2018), practices that also take place in India and the Philippines. According to the report, there is criminalisation of indigenous leaders and community members who voice opposition to projects related to extractive industries, agri-business, infrastructure, hydro-electric dams and logging. This process often leads to 'the prohibition of indigenous traditional livelihoods and the arrest, detention, forced eviction and violations of other human rights of indigenous peoples' (OHCHR 2018: 2). In the Philippines, for instance, one of the most prominent figures in the global movement for indigenous rights, Victoria Tauli-Corpuz, is included on a list of suspected terrorists by the government (Jacobson 2018). Recently, conservation projects have contributed to the worsening of indigenous human rights and many indigenous communities in Asia who rely on forests for their livelihood opposed conservation projects because the projects may convert their ancestral forests into protected areas. This can be seen, for instance, from the resistance of the Karen group in Tanintharyi Region, Myanmar, against the government's plan to establish a national park in their area in early 2018. The local communities say that the conservation plan would make it illegal for them to use forests within the designated area of the national park for their livelihood (Mon 2018). As the UN report states, 'indigenous people's ways of life and subsistence are deemed illegal or incompatible with conservation policies' (OHCHR 2018: 2).

2 Democratisation

2.1 National elections: Malaysia

The victory of the opposition Pakatan Harapan (PH) coalition party in the Malaysia national election held in May was a brief moment of hope for democracy and human rights in the region. The incumbent Barisan Nasional (BN) coalition had held power in various forms since Malaysia's independence in 1955. More recently its leader, Prime Minister Najib

Razak, has been questioned for corruption mainly involving the state sovereign wealth fund, 1MBD. The details of the corruption emerged in the previous years, with between \$4 to 5 billion taken from the 1MBD fund, and Razak himself having been found with \$600 million in his personal bank account. Investigations into this fund were started in several countries, including the United States, Singapore and Switzerland. Regardless of these irregularities there was no investigation in Malaysia, and members of parliament, including the Attorney-General, who raised concerns were dismissed or replaced. Efforts were made to keep this news from the Malaysian public, with a compliant national media not reporting on this story, and critical news media was closed, censored or banned. In the run-up to the elections attempts were made to gerrymander the results with the BN having smaller seats, and the opposition PH party voters corralled into seats sometimes twice as large as the average BN seat (Leong & Rodzi 2018). Further complaints were lodged about the overseas votes not being counted, ballot stuffing, vote buying, and the delay of the election results. Nevertheless, the opposition party won its first election.

While this presents much hope for democracy in the region, there are caveats. The opposition party won in part because it has Mohammed Mahathir as its leader, giving a safe choice for conservative Muslim voters not to vote for BN for the first time. Mahathir is an architect of the one-party dominant system during his over 20 years as leader of the BN. Further, he cannot be claimed as a defender of rights and democracy because of his well-known socially-conservative values and opposition to human rights. This is seen in subsequent actions regarding human rights in Malaysia since the election. Soon after the election there were moves to ratify human rights treaties, with the government initially saying it would ratify the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) and the Rome Statute. However, both these moves have been halted, primarily because of a campaign of misinformation by the ousted political parties. Malaysia currently has policies that give preference to ethnic Malays in some areas of education, land ownership, and business that were threatened to be taken away if ICERD was ratified. Most of the claims about ICERD were untrue, but the effective social media campaign, street protests, and support from pro-Malay and Islamic groups were too effective and the ruling party pulled out of signing ICERD by late 2018, and had withdrawn from agreeing to join the ICC by early 2019.

2.2 Other elections across the region: Bangladesh, Maldives, Cambodia and Timor Leste

A disturbing trend in the region is the manipulation of the election process by authoritarian regimes as they attempt to maintain power through unfair elections. The cases of the Bangladesh and Maldives national elections demonstrate this. Bangladesh completed its eleventh general election in December 2018, where Sheikh Hasina from Awami League was elected Prime Minister, but under questionable circumstances. Her chief rival, Khaleda Zia, leader of Bangladesh National Party (BNP), was barred from contesting the elections because of a corruption conviction and the opposition alliance, the Jatiya Oikya Front (National Unity Front) was successful in securing only eight of the 300 seats up for election. The chief of Bangladesh Election Commission denied any irregularities during the election, although reports tell another story. The election soon turned

hostile with security forces arresting and intimidating opposition figures and dissenting voices. Members and supporters of opposition parties were arrested, killed or disappeared with reports indicating the involvement of the ruling party in some of these incidents. The motorcade of opposition politician Dr Kamal Hossain was attacked, and between 9 and 12 December, 47 incidents of violence were reported in which eight people were killed and 560 were injured (OHCHR 2018). Although the right to vote and a free press are essential to democracy, these were not evident during the Bangladesh election. The replacement of the Information Communication Technology Act by the Digital Security Act (DSA) in October created restrictions on freedom of expression and prohibited investigative journalism that could have prevented rigging during the election. The Rapid Action Battalion (RAB)⁵ was tasked with monitoring social media for 'anti-state propaganda, rumours, fake news, and provocations' (HRW 2018c). The presence of election observers is important to ensure transparency. While they may not be able to stop the rigging of elections, they can point out existing irregularities. The Bangladesh government did not issue accreditations or visas within the timeframe necessary to conduct a credible international monitoring mission. Only seven of the 22 election non-governmental organisation (NGO) groups were approved to conduct domestic election observation (US Department of State 2018). The largest Asian independent election observing body ANFREL (Asian Network for Free Elections) terminated its decision to participate as observer because of significant delays in the accreditation approval by the Bangladesh Election Commission and visa approvals by the Ministry of Foreign Affairs (ANFREL 2018a). The 2018 elections marked the second lowest number of observers in two decades.

The 2018 Maldivian election took place among uncertainty and an unstable political landscape in the country, although there was 89,22 per cent voter turnout. Elections should give people a choice among candidates from various backgrounds, but this failed to materialise in the 2018 Maldivian election. In the run-up to the election, all opposition leaders were incarcerated through trials characterised as irregular and were barred from contesting in the election. This created obstacles to conduct fair and impartial elections since opposition candidates and parties did not have equal space and opportunity to access public facilities to organise their campaigns and political activities (Transparency Maldives 2019). ANFREL concluded that although the pre-election environment was systematically set up to favour the outgoing President, the issues observed on election day itself were not serious enough to impact the outcome of the election and called for an orderly transfer of power (ANFREL 2018b). The joint opposition candidate, Ibrahim Mohamed Solih, defeated then President Abdulla Yameen Abdul Gayoom by a wide margin in September 2018, but the outgoing President then attempted to sabotage the transfer of power. The outgoing President announced a state of emergency, suspending constitutional protections, banning public assemblies, and granting security forces sweeping powers to arrest and detain (HRW 2018d). These two examples of failed elections demonstrate the fragility of democracy in the region as entrenched interests attempt to maintain their power through manipulated election results.

5 The RAB is a paramilitary force implicated in serious human rights violations including extra-judicial killings and enforced disappearances.

National elections in several countries in Asia Pacific during 2018 show the strengthening of two phenomena: political violence and identity politics. In Cambodia political violence was intense during the election. The Cambodian government under Prime Minister Hun Sen arrested the leader of the main opposition party (Cambodia National Rescue Party/ CNRP) and dissolved it. Several political activists and the journalists who criticised Hun Sen were targeted for arrest and kidnapping. The government was also accused of involvement in four extra-judicial killings of activist and opposition members who challenged Hun Sen's leadership. This situation created fear and pressure among the Cambodian voters during the election. Without a genuine opposition, Cambodians were forced to vote for the ruling Cambodian People's Party (CPP). A HRW report details the extensive and systemic support of the military and police officers to mobilise votes for CPP in the election (HRW 2018b). As a result, CPP won all 125 National Assembly seats.

Another election in the Asia Pacific region took place in Timor Leste in 2018. Timor Leste conducted two elections within a year because the minority government of the 2017 election collapsed as the opposition thwarted the government's new budget proposal. In 2017 the Fretilin Party led by Prime Minister Alkatiri narrowly won a 0.2 per cent victory against the CNRT (National Congress for Timor Reconstruction), a party led by Xanana Gusmao. Timor Leste President Francisco 'Lu Olo' Guterres dissolved parliament in early 2018 and demanded another election. Xanana Gusmao's opposition coalition won the election. Even though the election was peaceful, there were cases of violence. Supporters of the Fretilin were in conflict with supporters of the AMP coalition party with 18 people injured and several vehicles burnt in violence in Baucau.

3 Update on regional bodies

3.1 Association of Southeast Asian Nations

Responses from ASEAN towards numerous crises and human rights violations in the region represent a weak and unreliable conflict resolution mechanism, known as 'constructive engagement'. While the responsible body in ASEAN, the ASEAN Intergovernmental Commission on Human Rights (AICHR) was established in 2009, and is known to have strong human rights advocates sitting as commissioners, it has yet to adopt significant and meaningful measures to solve the human rights crises throughout the region. There was a slight change in 2018 when ASEAN undertook its first activities: a visit to Myanmar and Bangladesh by an ASEAN delegation, and its humanitarian body, ASEAN humanitarian Assistance (AHA) was called upon to assist in repatriation. However, these measures were weak in comparison to the stronger response of individual members, most notably Malaysia and Indonesia (Tani 2018). This also reflected actions of AICHR, namely, strong responses from the Indonesian and Malaysia representatives, but no statements from the body itself. As in previous years, the norms of 'ASEAN way' have hampered the possibilities of member states to respond to human rights issues as the non-interference principle, which is rooted in the traditional concept of sovereignty, is not suitable to the current international and regional context, where AICHR has been active in working on the rights of persons with disabilities, and its thematic studies on legal aid, women affected by

natural disasters and juvenile justice. Studies and high-level meetings covered issues such as business and human rights, rights to water, and freedom of expression in the information age (AICHR 2018). AICHR also works alongside the Women and Children's Commission (ACWC) and the ASEAN Committee on Migrant Workers. While the ACWC remains an active body, the Committee on Migrant Workers, with only annual meetings, and quite divided support, has achieved little in its work over the past decade.

3.2 South Asian Association for Regional Cooperation

The South Asian Association for Regional Cooperation (SAARC), the regional body for India and its neighbours, has not established a regional human rights mechanism. The principle of non-interference and the exclusion of contentious issues found in article 2 of the SAARC Charter is one reason why this has not been done. The lack of unanimity on the part of the SAARC nations to hold an already-deferred SAARC summit exhibits the lack of urgency by this body to address critical issues surrounding South Asia. SAARC last met in 2014, and is next scheduled to meet in 2020, after the 2016 meeting was boycotted by India and four other nations. While there have been meetings of SAARC administrative bodies, there have been no activities around human rights. However, SAARC is slightly more active in the field of terrorism, which has long been of crucial importance in the region given that South Asia has been the hub of Islamist extremism. Terrorism in South Asia by radical Muslims has replaced insurgencies as the primary security concern, and this occurs in the context of two nuclear powers, India and Pakistan. For more than 20 years SAARC has been known to work on peace keeping, border security and law enforcement issues since it adopted a Regional Convention on the Suppression of Terrorism that called for cooperation among its member states on extradition, evidence sharing, and other information exchanges. A SAARC Terrorists Offences Monitoring Desk (STOMD) was also established for monitoring the Convention. However, sensitivities challenge the co-operation. Although experts in the region agree that trans-border terrorism and organised crime cannot be controlled without regional co-operation, it is difficult to get agreement within SAARC on such a sensitive matter. For example, Maoist insurgents now operating across the region share many features with the Indian Maoist insurgents, the Naxalites. However, Maoists in Nepal sit in government while those still active in Central Indian tribal hills are called terrorists by the Indian Prime Minister and are 'the biggest threat to national security'.

3.3 Pacific Island Forum

The Pacific Island Forum is dominated by issues of climate change and development, and there is no body dedicated to human rights. However, on its agenda are activities on domestic violence and gender equality. The Pacific Islands nations are some of the last to ratify CEDAW, mainly because of misbeliefs around abortion and same-sex marriage, but also because of strong opposition from Christian religious groups who are politically strong in the region (WUNRN 2016). Many Pacific Island political and legal systems favour males, with Tonga, for instance, allocating a plot of land to all males over the age of 16, without any similar benefit for women (WUNRN 2016). Human rights are part of the PIF foreign policy, with its interest in human rights in West Papua a concern

noted in the Communiqué resulting from the forty-ninth forum of the PIF in Nauru in September 2018. This is the only time human rights were mentioned in the 2018 Forum.

4 United Nations update

A number of core human rights conventions were ratified across the Asia Pacific. Fiji ratified both the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Cultural, Economic and Social Rights (ICESCR), and the Marshall Islands ratified ICESCR and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT). While this demonstrates advancements towards the universal acceptance of human rights, two sub-regions of the Asia Pacific lag behind the rest of the world as far as treaty ratification is concerned: Southeast Asia and the Pacific Islands. For Southeast Asia, the response is mixed with some countries with a near total ratification record, but Malaysia, Singapore and Brunei DS have ratified only two or three core treaties. Across the 14 Pacific Island countries, only one, the Marshall Islands, has ratified more than 10 conventions including optional protocols, and four have ratified fewer than four conventions. A notable event was the protests in Malaysia on the ratification of the ICERD treaty, detailed above in part 3.1. In South Asia many human rights treaties relevant to the region remain non-ratified. Although Nepal sends many migrant workers abroad, it is yet to ratify the Migrant Workers Convention. Bangladesh with systematic problems with enforced disappearances and ‘fake encounters’ is yet to ratify the Convention for Protection of All Persons from Enforced Disappearances, while Bhutan, which is praised in the world community for its environment-friendly policy (and being the only carbon-negative country) still has not ratified ICCPR or ICESCR.

During 2018 there were periodic reviews for China, Bangladesh and Malaysia. The Chinese review was noted for its politicisation, with pro-China countries taking up much of the review time (Worden 2018), and the Chinese delegation rejecting criticisms as ‘politically driven’ (Kuo 2018). China supported 207 out of 284 recommendations (although it must be remembered that many recommending states were politically allied to China). The Bangladesh government accepted 167 of the 251 recommendations, although it refused to accept recommendations on the death penalty, LGBT rights and the ratification of treaties (*Dhaka Tribune* 2018; FIDH 2018). For the Asia Pacific the other significant events at the UN for the Asia Pacific were the findings of the fact-finding mission in Myanmar (described in part 1.1).

A number of important actions at the UN level occurred in 2018 in relation to migration and climate change. The Global Compact for Safe, Orderly and Regular Migration (GCM) was accepted on 10 December (Human Rights Day), and plans to implement the Paris Agreement on climate change (COP 24) were made in Poland on 15 December. The GCM did not receive universal support with five states voting against, and 12 abstaining (mainly from Europe), although the resolution passed with 164 states agreeing to the document. The trend is for governments to oppose migration, with some European states taking strong anti-immigration stances. It should be noted that from the Asia Pacific only

North Korea and Afghanistan did not vote. All countries supported the COP 24 document, but many important and difficult issues were left out of the agreement because of a lack of agreement between the participants (Carbon Brief 2018). Similarly, many states are not strongly committed to counter climate change and unwilling to make financial and policy commitments to reducing carbon emissions. In the Asia Pacific region there is strong support for countering climate change, with the Pacific Islands leading the advocacy. As the Pacific Small Island Developing States declared in their Statement before COP 24 (COP 23 Fiji 2018):

We firmly believe that the COP24 ... is a pivotal moment in human history. The world must take heed of the Intergovernmental Panel on Climate Change (IPCC) Special Report on the impacts of global warming ... and take dramatic and urgent steps to decarbonise the global economy and assist those at the frontline of climate change impacts. Our future is at stake.

Even China was noted to have changed its position from recalcitrance to support of combating climate change (Hartzell 2019). It is somewhat reassuring that in these two important areas there is a support across the Asia Pacific. However, similar widespread support for human rights and democratisation is yet to be found. The region is willing to invest in problems that it sees as immediate and relevant, but not yet to put in place a longer-term infrastructure of human rights and the rule of law. The systemic problems of reduced political freedoms and discrimination are yet to be solved. While the year 2018 did not see the plummeting of rights that occurred in 2016 and 2017, there were no major reversals of human rights standards. Matters have not worsened, but they have also not improved.

References

- ABC 'Malaysia's Mahathir Mohamad warns against "new colonialism" during China visit' Australia ABC 21 August 2018, available at <https://www.abc.net.au/news/2018-08-21/mahathir-says-china-will-sympathise-with-malaysia-problems/10145750> (last visited 31 October 2019)
- AICHR Annual Report 2018 Jakarta: ASEAN Intergovernmental Commission on Human Rights
- Amnesty International (2018a) 'We will destroy everything': Military Responsibility for Crimes against Humanity in Rakhine State Report, London: Amnesty International, 27 June 2018
- Amnesty International (2018b) Annual Report 2017-2018 London: Amnesty International
- ANFREL (2018a) 'ANFREL statement on the termination of its mission on Bangladesh' Bangkok: ANFREL, 23 December 2018, available at <https://anfrel.org/anfrel-statement-on-the-termination-of-its-mission-in-bangladesh/> (last visited 31 October 2019)
- ANFREL (2018b) 'Transparency Maldives call on all parties to uphold the will of the people and facilitate a peaceful transfer of power' Statement Bangkok: ANFREL, 14 September 2018

- APCR2P 'December 2018: Risk Assessment Series Vol 8: Indonesia' Brisbane: Asia-Pacific Centre for the Responsibility to Protect, December 2018
- BBC Trending 'The country where Facebook posts whipped up hate' London: BBC 12 September 2008, available at <https://www.bbc.com/news/blogs-trending-45449938> (last visited 31 October 2019)
- Bengwayan MA (2003) *Intellectual and cultural property rights of indigenous and tribal peoples in Asia* London: Minority Rights Group International
- Burlie JA (2008) *The Burmanisation of Myanmar's Muslims* Bangkok: White Lotus Press
- Carbon Brief 2018 'COP24: Key outcomes agreed at the UN climate talks in Katowice' 16 December 2018, available at <https://www.carbonbrief.org/cop24-key-outcomes-agreed-at-the-un-climate-talks-in-katowice> (last visited 31 October 2019)
- Coconuts Bangkok 'Misogynist military boss: Prayuth says gender equality "will make Thai society deteriorate"' Coconuts Bangkok 1 February 2016, available at <https://coconuts.co/bangkok/news/misogynist-military-boss-prayuth-says-gender-equality-will-make-thai-society-deteriorate/> (last visited 31 October 2019)
- COP 23 Fiji 'Pacific Small Island developing states appeal for universal support for IPCC Special Report' Fiji: COP23 13 December 2018, available at <https://cop23.com.fj/pacific-small-island-developing-states-appeal-universal-support-ipcc-special-report/> (last visited 31 October 2019)
- Dhaka Tribune 'Govt rejects UPR recommendations on media law, death penalty, LGBT rights' Dhaka: *Dhaka Tribune*, 18 May 2018
- Engle K 'On fragile architecture: The UN Declaration on the Rights of Indigenous Peoples in the context of human rights' (2011) 22 *European Journal of International Law* 141
- FIDH 'Government shows lack of commitment to address serious human rights violations during UN review' Press Release Paris: FIDH 18 May 2018
- Goldberg J 'Hope fades: Posters of Aung San Suu Kyi gather dust as image tarnishes' *Guardian* 12 September 2018
- Hartzell L 'A shift in climate strategy: China at the COP 24' Blog post: China USA Focus, 25 January 2019
- Haynes S 'Two more medical schools in Japan have admitted to discriminating against women' *Time* 12 December 2018, available at <https://time.com/5477556/japan-medical-school-discrimination-new-cases/> (last visited 31 October 2019)
- HRW 'China: Free Xinjiang "political education" detainees' Press Release New York: HRW 10 September 2017
- HRW (2018a) 'Bangladesh is not my country': The plight of Rohingya refugees from Myanmar. Report New York: Human Rights Watch, 5 August 2018
- HRW (2018b) 'Cambodia: July 29 elections not genuine' Press Release New York, Human Rights Watch 25 July 2018
- HRW (2018c) '"Creating panic": Bangladesh election crackdown on political opponents and critics' Report New York, Human Rights Watch, 22 December 2018
- HRW (2018d) 'Maldives: Election rigging feared: New rules threaten free vote on September 23' Press Release New York, Human Rights Watch 19 September 2018
- HRW (2019a) World Report 2019. Annual Report New York: Human Rights Watch

- HRW (2019b) 'Indonesia: Inadequate efforts to curb intolerance: Religious, gender minorities face persistent harassment' Press Release New York: Human Rights Watch 17 January 2019
- Human Rights Council Report of the independent international fact-finding mission on Myanmar 39th session, 10-28 September 2018 A/HR/39/64
- Jacobson P 'UN's Tauli Corpuz accused of terrorism in her native Philippines.' *Mongabay* 20 March 2018
- Jiang S 'Thousands of Uyghur Muslims detained in Chinese "political education" camps' CNN 3 February 2018, available at <https://edition.cnn.com/2018/02/02/asia/china-xinjiang-detention-camps-intl/index.html> (last visited 31 October 2019)
- Kuo L 'China says UN criticism of human rights record is "politically driven"' *The Guardian* 7 November 2019
- Leong T & Rodzi N 'Electoral maps for upcoming Malaysia election passed in Parliament' *The Straits Times* 28 March 2018
- McCurry Justin 'Two more Japanese medical schools admit discriminating against women' *Guardian* 2 December 2018
- Millar Alistair 'Developing regional counter-terrorism cooperation in South Asia' *CTC Sentinel* 12 December 2009 18
- Mon Su M 'Karen group says plan to protect forests ignores people's rights' *Frontier Myanmar* 11 April 2018
- Mozur P 'A genocide incited on Facebook, with posts from Myanmar's military' *New York Times* 16 October 2018
- Nathani K 'China considers law against sexual harassment at workplace' *Entrepreneur Asia Pacific* 28 August 2018
- OHCHR 2018 'Report of the Special Rapporteur on the Rights of Indigenous Peoples' Geenva: OHCHR: HRC/SR/A.HRC.39
- Radcliffe SA 'Geography and indigeneity III: Co-articulation of colonialism and capitalism in indigeneity's economies' *Progress in Human Geography* 5 February 2019
- Repnikova M & Weile Z '#MeToo movement in China: Powerful yet fragile' *Aljazeera* 23 October 2018, available at <https://www.aljazeera.com/indepth/opinion/metoo-movement-china-powerful-fragile-181022082126244.html> (last visited 31 October 2019)
- Secretary-General 'Secretary-General's remarks to the Security Council on Myanmar' New York: UN Secretary-General 28 August 2018, available at <https://www.un.org/sg/en/content/sg/statement/2018-08-28/secretary-generals-remarks-security-council-myanmar-delivered> (last visited 31 October 2019)
- Soe Khin H 'Burma's sexist school requirements hurt women – and society' *Irrawaddy* 7 September 2014, available at <https://www.irrawaddy.com/specials/women/burmas-sexist-school-requirements-hurt-women-society.html> (last visited 31 October 2019)
- Stewart P 'China putting minority Muslims in "concentration camps", US says' *Reuters* 4 May 2019
- Suryadinata L 'Pancasila and the challenge of political Islam: Past and present' *Trends in Southeast Asia* 14. Singapore ISEAS 2018
- Synopsis & Jichang L 'United Nations with Chinese characteristics: Elite capture and discourse management on a global scale' *Synopsis* 25 June 2018, available at <https://synopsis.cz/en/united-nations-with-chinese-characteristics-elite-capture-and-discourse-management-on-a-global-scale/> (last visited 31 October 2019)

- Tani M 'ASEAN aims to express "concern" on Rohingya crisis for first time' *Nikkei Asian Review* 13 November 2018
- Transparency Maldives 'Election Observation Report: Presidential Election 2018' Mali: Transparency Maldives, 28 March 2019
- UNOHCHR 'Bangladesh: UN human rights experts alarmed by violence ahead of election' Press release Geneva: United Nations Office of the High Commissioner of Human Rights, 20 December 2018
- USCIRF 2019 Annual Report 2018. Washington: US Commission for International Religious Freedom
- US Department of State 2018 Country reports on Human Rights Practices for 2018 Washington: United States Department of State, Bureau of Democracy Human Rights and Labor
- Wahid Foundation National Survey 2016: A measure of the extent of socio-religious intolerance and radicalism within Muslim society in Indonesia Jakarta: Wahid Foundation, 18 October 2017
- WUNRN 'Tonga – Ongoing debate over CEDAW ratification, reflects US CEDAW challenges on a smaller scale' Women's UN Report Network 1 February 2016, available at <https://wunrn.com/2016/02/tonga-ongoing-debate-over-cedaw-ratification-reflects-us-cedaw-challenges-on-a-smaller-scale/>
- Worden, Andrea 2018. 'China Deals Another Blow to the International Human Rights Framework at its UN Universal Periodic Review.' Blog Post. *China Change*, November 25, <https://chinachange.org/2018/11/25/china-deals-another-blow-to-the-international-human-rights-framework-at-its-un-universal-periodic-review/> (last visited 31 October 2019)
- Zheng S 'The fight against gender violence goes on for China's "feminist five"' *South China Morning Post* 14 May 2017

Child protection and EU cooperation between Eastern Partnership countries during 2018, with a focus on Armenia, Georgia and Ukraine

Mariam Muradyan*

Abstract: This is a brief overview of progress and challenges in three Eastern Partnership (EaP) countries during 2018. The first part of the article analyses the commitments and obligations of three EaP countries under the international and regional frameworks, emphasising the relevant mechanisms and checks and balances. In this part the United Nations and Council of Europe mechanisms are considered. The cooperation framework between the European Union (EU) and the EaP countries is considered separately. Considering the fact that human rights protection has always been one of the key preconditions in developing political and economic cooperation between the EU and partner countries and the fact that the EU proclaims itself as a global actor, human rights and child protection are considered separate cooperation dimensions. In the second part the bilateral and multilateral cooperation with the EaP countries is categorised into three clauses. The clauses are built on the announced strategies and agendas of cooperation emphasising the slight deviations from the initial plans. Furthermore, the overview of selected achievements and perplexing challenges in human rights with the focus on child protection are described in Armenia, Georgia and Ukraine. Although some comparisons are drawn between the three countries, the contribution encourages the idea of considering each country individually bearing in mind the recent changes in political transformation both in domestic and international relations, economic declines and social transformations caused by the aftermath of the conflicts with Russia, as well as the advancements in fulfilling the bilateral agendas. The research shows that the announced targets and the EU's commitments and actions in developing national judiciary, human rights protection and social systems in Armenia, Georgia and Ukraine are slow. Nevertheless, the delayed achievements in human rights and child protection do not hinder the nature of cooperation between the EU and EaP countries, displaying the weak connection of human rights conditionality in the external policy of the EU with its neighbours.

Key words: human rights; child protection; European Union; Eastern Partnership; partnership clauses

* (Child Rights and EU Studies) (Yerevan State University, Armenia), Child Rights Researcher and Practitioner on Child Protection and Child-Related Policies email

1 Introduction

This article is built on three main questions: What are the challenges and what progress has been made during 2018 in the Eastern Partnership (EaP) countries, namely, Armenia, Georgia and Ukraine? What are the commitments of the European Union (EU) to human rights protection in these countries? What, more specifically, is its contribution to the field of child protection? The research objectives derive from the legal documents (partnership agreements, action plans and support frameworks concluded between the EU and Armenia, Georgia and Ukraine) and from the studies of children's rights conducted and evaluated by national and international non-governmental organisations (NGOs). The article considers the human rights commitments of the EU in general, and its interests, strategies and scope of engagement as a global actor in promotion and protection of children's rights. Furthermore, the landscape of child protection issues in the three countries is briefly elaborated upon, amplified by the EU's support in each country in that regard. The bilateral cooperation concluded between the EU and EaP countries is categorised on the basis of the country experiences with these partnership clauses, described here as 'muddling through' clauses, the 'outlier' clauses and the 'unconditional love' clauses. These agreements demonstrate that although a unified framework initially regulated the EU's cooperation with EaP countries, recent developments in respect of political, social and economic transformation in the three countries demanded an individual approach for each. Therefore, although some comparative analysis is undertaken, based on the Soviet legacy shared by Armenia, Georgia and Ukraine, the research is largely country-specific since there are relatively few similarities in the political systems and obligations derived from the international treaties to which the three countries are party.

2 International and regional frameworks on human rights and child protection

The international institution for the protection of children's rights constitutes a system of principles and norms that determines the rights and freedoms of children. It establishes the duties of states to secure and implement them, and also defines an array of international monitoring measures to secure proper implementation of the obligations under the treaties to which these states are party. Notwithstanding challenges such as poverty and a low level of development of states parties, their governments are obliged to create or reinforce the existing national or local judicial, institutional or systemic environment and to protect children against any form of exploitation and violence, abuse or harmful labour, and prevent children from being separated from their families against their will.

2.1 International standards

The Convention on the Rights of the Child (CRC) remains the most comprehensive international treaty on the rights of children, their protection and the corresponding obligations of state parties. The rights of the child may be categorised into three groups, namely (i) survival and development rights (for instance, parental guidance, survival and development, rights on registration, name, nationality, care, and

preservation of identity) (CRC arts 4-10, 14, 18, 20, 22-31); (ii) participation rights (CRC arts 12-15 on respect of the views of the child, freedom of expression, thought, conscience, religion and association); and (iii) protection rights. Article 4 of CRC provides that governments must undertake 'all appropriate measures' available at the state level for respect for, the protection and fulfilment of children's rights. 'All appropriate measures' in this regard are considered to be the social, legal, health and educational services, as well as the systems of their review and assessment, for implementing the minimum standards of child protection, further elaborated in the Optional Protocols to CRC.¹

ILO Convention 182 of 1999 lists the 'worst forms of labour' such as slavery, the sale and trafficking of children, child prostitution and the recruitment of children into harmful activities such as drug dealing, the production of pornography, and compulsory enrolment as child soldier (ILO Convention 182: art 3). Sexual exploitation, child prostitution and pornography have been augmented in the Second Optional Protocol to CRC. This Protocol recognises the importance and promotes the implementation of the principles, commitment and the agenda for actions adopted at the World Congress against Commercial Sexual Exploitation of Children, held in 1996 (UNGA 2002). The ILO Convention condemns children's exploitation for remuneration, the transfer of organs, child prostitution and the engagement of children in forced labour (arts 2 & 3(c)).

The protection of the child's interests through family law is also provided for in the International Covenant on Civil and Political Rights (ICCPR). Among these clauses are limitations on a court to publicise proceedings concerning 'matrimonial disputes or the guardianship of the children' (art 14(1)); 'the respect for liberty of parents and legal guardians for undertaking religious and moral education' (art 18(4)); protection of children in case of divorce (art 23(4)); as well as the right of the child to be protected as 'a part of a family, society and the state', and to be 'registered at the time of birth and acquire nationality' (art 24). Other social rights of children are mentioned in the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) (arts 5(b), 9(2), 11 & 16).

Some non-legally-binding international standards for the protection of children from poverty, hunger and the provision of good health conditions and quality education are stipulated in the UN 2030 Agenda for Sustainable Development (UNGA 2015). The entitlement to do so, particularly financing aspects for development, was stated in the Addis Ababa Action Agenda (UN Addis Ababa Action Agenda 2015).

2.2 Council of Europe standards

Child protection is not considered a fundamental value of the Council of Europe (CoE), but instead is mentioned as one of the key areas of its work in its campaigns, projects and legal documents. The comprehensive

1 There are three Optional Protocols to the Convention: the Optional Protocol (1) on the Sale of Children, Child Prostitution and Child Pornography; (2) on the Involvement of Children in Armed Conflict; and (3) on the Communication Procedure. The latter has only 29 state parties whereas the first (173 countries) and the second (165 countries) protocols are more integrated.

approach to child protection standards is conveyed in the 1950 European Convention on Human Rights and Fundamental Freedoms (European Convention), which defines the human rights standards, freedoms and obligations of state parties. Most of the Convention provisions target the human being as a bearer of stipulated rights, thus adhering also to the rights and freedoms of children: the rights to respect private and family life; fair trial; liberty and security; prohibition of torture; and freedom of thought, conscience and religion. The European Convention establishes the European Court of Human Rights (European Court) as the only regional judicial remedy for individuals whose human rights have been violated. Based on its case law, the European Court made a distinction between 'procedural' and 'substantive' state obligations (Kombe 2007: 18).

The Convention mentions 'child', 'minor' or 'juvenile' only in three articles: deprivation of the liberty by detaining with the 'educational supervision or with the purpose to bring the minor in front of a competent legal authority' (art 51(d)); the 'right to a fair trial' defining the right of everyone to a fair and public hearing, pronouncing the judgment concerning juveniles is a limitation to the court art 6(1)). There is no specific provision on child protection in the ECHR, but it provides for the rights of general applicability such as the prohibition of slavery and forced labour, torture, rights to a fair trial and an effective remedy and other social and political rights.

The European Social Charter (Charter) was a revival of the social and protection rights and a contribution to the child protection framework within the Council. Among the contributions of the Charter, there are the rights to 'protection from sexual harassment in the workplace' and other forms of harassment (art 26); the right of workers with family responsibilities to 'equal opportunities and equal treatment' (art 27); and the right to 'protection against poverty and social inclusion' (art 30).

For the development of national strategies, the Council established Policy Guidelines on Integrated National Strategies for the Protection of Children from Violence (Council of Europe Policy Guidelines 2009). It proposes a holistic multidisciplinary and systematic framework to be adopted by member states to eradicate and respond to all acts of violence towards children. The third CoE strategy of 2016 on children's rights proposes a systematic and measurable approach based on the impact and outcome principle, evaluated once every three years. The CoE Strategy for the Rights of the Child (2016-2021) highlights five priority areas (Council of Europe Strategy for the Rights of the Child 2006): equal opportunities; participation of children; a life free from violence; child-friendly justice; and children's rights in the digital environment.

The CoE inherited the international principles on child protection mainly from the Universal Declaration of Human Rights (Universal Declaration) and CRC. The added value in the principles and standards are those relating to a more specific target group, for instance children as victims of domestic violence. However, the CoE contribution is paramount in proposing measures and tools for developing domestic and national mechanisms for child protection areas. Although the Convention and the Social Charter are legally binding, unlike the EU, the CoE lacks political conditionality, resulting in limits to its ability to efficiently and promptly leverage implementation and monitoring.

2.3 European Union standards

The Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) in several clauses refer to human rights. Nevertheless, the Charter of Fundamental Rights of the European Union adopted by the proclamation of Nice European Council in 2000 is the main source of human rights within the EU. The Charter became binding after nine years with slight amendments brought about by the Lisbon Treaty. In 2000 the document was not perceived as part of the EU legal order; but was viewed as a catalogue of fundamental rights supplementing the *acquis* of the EU legal order. Article 6(1) of the TEU 'recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union' (EU 'Lisbon' 2016: art 6(1)) TEU). Article 6(2) links the Union with the European Convention within the competences of the EU stated in the Treaties (EU 'Lisbon' 2016: art 6(2) TEU).

Human rights as a principle of the EU was especially pivotal in the 2004 and 2007 enlargements, when the new member states that joined the EU were radically different from the conventional member states of the Community. Such a transformation of the EU with the normative convergence of post-Communist states was supposed to be safeguarded by various monitoring and observance tools harnessed by the European Commission. Respect for human rights later on became one of the key priority areas in multilateral and bilateral relations between the EU and its neighbours and partners.

The TEU, the TFEU and the Charter refer to the rights of children through general and specific aspects. Article 3(5) of the TEU mentions the protection of human rights, and particularly the rights of the child, among the EU's general goals to promote human rights values in relation to the wider world (EU 'Lisbon' 2016: art 3(1) TEU). In the TFEU, children are considered in the framework of the provisions devoted to citizenship (EU 'Lisbon' 2016: art 83(1) TEU), in measures to combat trafficking in women and children (EU 'Lisbon' 2016: art 79(2)(d) TEU), and in cross-border crimes (EU 'Lisbon' 2016: art 83(1) TEU). Only the Charter, in article 24 on 'The Right of the Child', refers to children as separate rights holders. It highlights the importance of deliberating the best interests of the child primarily in 'all actions related to children' (EU Charter 2016: art 24(2)), and considers the issue of the child's personal relations with parents, with certain limitations (EU Charter 2016: art 24(3)).

Three main documents, adopted by the EU, are important in operationalising child rights: the EU Strategy on the Rights of the Child (2006); the EU Agenda for the Rights of the Child (2011); and the EU Guidelines for the Promotion and Protection of the Rights of the Child (2007 and 2017). The last document suggests practical approaches for promoting, protecting and fulfilling children's rights in the EU's external actions. Among the operational tools, the EU promotes political dialogue, demarches, bi- and multi-lateral cooperation and partnership with international stakeholders to intensify coordination of concerted efforts in the field.

The UN Sustainable Development Goals 2030, a consequence of the refugee crisis of 2015 causing massive children's rights violations, coupled with the EU's commitment 'to leave no child behind' (EU Guidelines 2017: 3), fostered the EU's engagement in protection of children's rights. Particularly, in October 2016 the EU delegation to the UN announced, on behalf of the EU and its member states, that the EU was planning to become a major player in and contributor to the promotion and protection of the rights of children (EU Statement 2016). The Statement was followed by the updated EU Child Protection Guidelines, published in February 2017. The updated Guidelines intensify the rights-based approach and promote the concept of a 'system strengthening approach' (CRC General Comment 5).

3 The European Union human rights frameworks with European neighbourhood countries

One of the reasons for the EU not initially considering human rights its primary responsibility was the fact that a human rights-based regional organisation already existed in Europe. Human rights were considered as falling in the remit of the CoE rather than the EU, which instead was perceived as achieving political and economic objectives. Some member states such as Germany considered fundamental human rights as part of the 'general principles of community law', thus European Community law was not supposed to prevail over the fundamental guarantees of the German basic law (Craig & De Burca 2003: 269).

As mentioned, the culture of fundamental rights in the EU was adopted with the proclamation of the Charter of Fundamental Rights and the vitality of the Charter was affirmed in the law and policy making of the EU institutions. Although 'the Parliament, the Commission and the Council [should] jointly and formally recognise the existence of positive obligations to protect and promote human rights as a part of EU law' (European Commission 2012), there is no clear guidance about aligning domestic laws and policies with the Charter. Such an institutional guidance is provided by the European Union Agency for Fundamental Rights (FRA) and the European Ombudsman.

Within the bilateral track, cooperation in the field of human rights was enforced through particular instruments after the launch of the European Neighbourhood Policy (ENP) in 2004 and the Eastern Partnership in 2009.

With the extension of the ENP into the EaP of South Caucasus, the partner governments agreed on mentioning the priorities and setting the agenda in the Action Plans. The ENP includes conditionality, joint ownership, regional cooperation and deeper integration. The policy was based on the values and criteria suggested in 1993 to those willing to become member of the European Community. Both the European Neighbourhood Policy and the Copenhagen criteria restated the mandatory need of states to demonstrate political stability through institutions, guaranteeing democracy, the rule of law and human rights as prerequisites for joining the EC. The EaP is based on mutual commitment to the rule of law, good governance, respect for human rights, respect for

the protection of minorities and the principle of market economy and sustainable development.

The EU and its eastern neighbours cooperate through the establishment of multi- and bilateral tracks and various tools and projects. The bilateral track consists of Association Agreements (AA) and Deep and Comprehensive Free Trade Agreements (DCFTAs). The DCFTAs provide for convergence with the EU laws and standards of positive effects of the trade, investment liberalisation and energy security. The multilateral dimension added two more platforms, namely, (i) democracy, good governance and stability; and (ii) contact between people. Despite this framework, the question is whether the EU's political and economic interests in the region overshadows its commitment to human rights protection in the neighbourhood. Questions remain as the extent to which the EU remains vigilant to human rights advocacy in a context in which many other imperatives are at play. While the EU aims to achieve deeper and more comprehensive collaboration with EaP countries, the question arises why human rights are often neglected despite the framework for cooperation being so clearly based on human rights.

Part of the answer lies in the direct connection of these eastern countries with Russia. The EU's priority to forge a common bond based on mutual interest and stronger economic partnership with EaP countries has to a large extent overridden concern for human rights issues.

Regardless the universality of human rights promoted by UN throughout the world, the EU's interest and involvement in human rights protection is directly proportionate to the foreign policy of the countries. Over time, the European Council's agenda embraced more than economic unity, and shifted towards more political objectives. Human rights and democracy were for example included in the Common Foreign and Security Policy (CFSP). The Council's Resolution of November 1991 remains central in this policy area. It provides for financial resources to stimulate respect for human rights ('carrot'-provisions), and restrictive measures for the violation of human rights ('stick'-provisions). Different formulas have been adopted based on the communications of the Commission upon the agreements, differing from country to country in respect of the degree of harshness and flexibility. The following formulas are central while considering the EU's engagement with and interest in the human rights field of countries in this region: (i) 'democratic principle' clause – the list of concerns applied first to Latin American countries entailed the respect of democratic principles and human rights; (ii) 'essential element clause' – suggesting the insertion of a suspension mechanism with necessary legal bases provided by the Vienna Convention; (iii) the previously 'suspension' or 'Baltic clause' for suspending the agreement wholly or in part; and (iv) 'non-performance' or 'non-execution' clause.

These clauses were applied in relation to democratic and human rights principles to countries that are became members of the EU. The development of partnerships took the same path and entailed some of these clauses at the preliminary stage. Human rights protection was considered as a central issue with partners. However, in this article, the impact of three other clauses – the 'muddling through', 'outlier' and 'unconditional love' clauses – are also considered.

'Muddling through' clause: This kind of clause refers to the comprehensiveness and limitlessness of the EU partnership and foreign policy tools. Association agreements are the main legal tools to secure partnership with neighbours. Their content is quite comprehensive and is based on shared values and principles, in particular democracy, the rule of law, respect for human rights and fundamental freedoms, good governance market economy and sustainable development. As for the global strategy of the EU's foreign and security policy, it concentrates on security issues exercised in broader partnership, values, variety of stakeholders and partners involved. Conversion from partnering into a joint union, which supposes its participation in shaping agenda, represents the unit as a partnership both with states and individual units, private and civil sectors, as well as for the UN and other regional organisations. Such representation is possible if the understanding of values and goals of the unit are clear and admissible for the members of the unit themselves.

'Outlier' clause: These clauses mainly refer to EaP countries – Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. Agreements with Belarus and Azerbaijan do not contain free trade agreements, as they are not members of the WTO. The main goals of these clauses are to accelerate political association and further economic integration between the EU and the EaP through DCFTAs as part of broader political AAs. The process was hampered by political crises. The EaP Summit in Vilnius in November 2013 was supposed to be the venue for signing AAs including the DCFT, with Ukraine, and for initiating similar agreements with Armenia, Georgia and Moldova. However, this attempt at EU penetration in the region provoked turmoil in the Kremlin. The Eurasian Customs Union (now the Eurasian Economic Union) was initially composed of Russia, Belarus and Kazakhstan, thus excluding Armenia, Georgia or Ukraine. In November 2013, facing strong Russian pressure, Ukrainian President Yanukovich decided to suspend preparations for the signing of the EU-Ukraine Association Agreement. In September 2013, Armenia decided to join the Russian-led initiative, thus declining the signing of its Association Agreement with the EU. In 2015, Armenia formally became part of the Eurasian Economic Union.

'Unconditional love' clause: One of the driving forces of the ENP launch was to resolve instability in the region and to provide an economic vision, for instance, for energy security the EU planned to open a direct route to Central Asia. Even if promoting European democratic values was quite central for the EU, it bent backwards to accommodate partners who were central to realise this vision. In some partnership countries such as Belarus and Azerbaijan, its 'unconditional love' appears from the dominance of the 'carrot' above the 'stick'-approach despite the existence of notable human rights violations.

With the EU's 'new response to a changing neighbourhood', the ENP countries were bound by the new approach. According to these commitments the EU will support building democracy to ensure the fulfilment of basic political, social and human rights, support inclusive economic development and the strengthening of more consistent regional initiatives in certain areas covering the EaP and the Southern

Mediterranean, as well as mechanisms and instruments for implementing these objectives.²

4 Child protection in Eastern Partnership countries

4.1 Armenia

Armenia ratified CRC in 1993. In 2005 Armenia ratified two Optional Protocols to CRC, namely, ILO Convention 182 and the Hague Convention on Protection of Children and the Cooperation in Respect of Intercountry Adoption. Among state obligations underlying in the treaties there is an obligation to amend legislation and policy towards the improvement of child protection in Armenia. In 1996 through the Law of the Republic of Armenia on Child's Rights,³ Armenia adopted regulations pertaining to the public sector and determined the priority of the international law over domestic laws.

The Criminal Code envisages clauses related to the violation of certain standards of child protection, such as kidnapping (Armenian Criminal Code art 131(1)), any enrolment of the child into antisocial activities (Armenian Criminal Code art 166(1)), and child trafficking (Armenian Criminal Code art 168). There are certain discrepancies between the Law on the Child's Rights and the Criminal Code. For example, the Criminal Code provides for mitigated punishment in respect of children under 14 years of age (Armenian Criminal Code art 62(1)(4)), while the Law on the Child's Rights defines a 'child' as anyone under the age of 18. There is therefore some uncertainty about the punishment of persons 15 to 18 years old.

The Permanent Body in Parliament, the office of the Ombudsman and the Commission on the Protection of the Child's Rights are tasked with the implementation of relevant policies and laws. The Commission also secures the enrolment of the civil society representatives in the drafting and implementation of national policies.

The first Strategic Plan of 2004-2015 on the Protection of the Rights of the Child established a three-tier child protection system.⁴ The system distributes obligations of the state into national, regional and community levels. However, the Government Decree determining the functions and obligations of authorities at each level, later superseded by another decree, does not provide solid grounds for efficient protection.⁵

2 EUR-Lex, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A new repose to a changing Neighborhood/*COM/2011/0303 final*/, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011DC0303> (last visited 1 April 2017).

3 National Assembly of Republic of Armenia, The Law of the Republic of Armenia on the Child's Rights, May 29, 1996, non-official translation, available at <http://www.ombuds.am/resources/ombudsman/uploads/files/agreements/2d25331b2ad440a56d9e450a307813f3.pdf> (last visited 30 March 2017).

4 Government of Republic of Armenia, Decree 1745 of 18 December 2003 on Adopting Child Protection National Plan of 2004-2015, Yerevan, 2003, Ch II, art 4.

5 Government of Republic of Armenia, Decree 1694 of 27 December 2012 on Protection of the Child Rights Strategic Plan of 2013-2016 and Approval of the Agenda of 2013-2016 Strategic Plan and Recognising the Decree N1745 of December 18 Invalid, Yerevan, 2012.

The absence of efficient data recruitment and database backup for children at risk or child cases by any of the institutions from three-tier protection constitutes another challenge.⁶ The integrated social services, first launched in 2012 and extended in 2014, were considered to address the gaps in the previous systems. The system is defined 'as 'a complex of tasks (responsibilities) and events performed by state and local government bodies, organisations and individuals performed within the social support framework'.⁷

The Child Protection Strategy of 2017-2021 highlights the necessity of improved principles and criteria of providing alternative care (implementation and increase of fostering families), capacity-building events for social workers within the implementation of the integrated social service system.⁸ It emphasises the necessity of enforcing the child protection system through a comprehensive child protection database, to create specialised services and mechanisms for preventing violence against children, operative and coordinated mechanisms for fulfilling the needs of child victims of armed conflicts, and children living in extremely difficult conditions and refugee children.⁹

Thus, although the legal framework and the systemic approach to the protection of the rights of the child are established, Armenia remains behind with the implementation of its announced strategy. According to the Child Labour National Study of 2016, among the interviewed 453 000 children of ages five to 17 years, 11,5 per cent were engaged in labour (52 000 children) and 9 per cent (39 300 children) were engaged in labour that posed physical, social and moral hazards to children.¹⁰ According to the Child Protection Index 2016, compared to the eight other countries reviewed, Armenia performs well at the law and policy level, but has the lowest scores on the indicator of economic exploitation and violence against children.¹¹

The Armenian Ombudsman in the 2018 *Ad Hoc* Public Report on the Status of Commitments under the CRC and Its Optional Protocols reviewed the implementation period from January 2013 to December 2017. It considers the need to review the Armenian strategy on child

6 Government of Republic of Armenia, Decree 1273 of the Government of the RA on Amendments in Decree 1694 of the Government of RA, Yerevan, November 2014, art 18.

7 RA, the Law of the RA on Social Support, adopted 17 December of 2014, Chapter 7 System of Social Support Services, Social Cooperation and Local Social Projects, Yerevan, 2014, art 33(1).

8 Government of Republic of Armenia, Draft of the RA Decree on Child Protection Strategy of 2017-2021 and Action Plan of Child Protection Strategy 2017-2021, Ch VII, available at <http://www.mlsa.am/forum/forum.php?sec=conference> (last visited 30 March 2017).

9 Ch IX, art 30.

10 State Statistics Service of Republic of Armenia, Child Labour State Study 2015 12, available at <http://www.armstat.am/file/doc/99499668.pdf> (last visited 2 April 2017).

11 Child Protection Network (CPN) with the national coordination in nine countries evaluates the child protection systems to improve the protection and well-being of children. It is designed to encourage regional cooperation, stimulate better implementation of the UNCRC, and serve as a policy analysis tool for civil society governments and donors. Armenian Child Protection Network, Child Protection Index Armenia 2016, available at <http://2016.childprotectionindex.org/country/armenia> (last visited 15 February 2017).

protection and the effectiveness of its implementing mechanisms.¹² It found that there were no progress in health and education allocations since 2013, where the threshold on health was 1,5 per cent and 2,34 per cent of the gross domestic product (GDP) on education.¹³

Armenia announced the National Programme to attempt improving the quality of children's lives. The bold priorities are children who live in families; children who receive adequate health, education and protection services. However, in the process of creating such systems, 'even the services intended to secure equal rights and opportunities for children in difficult situations, are mostly guided by the needs rather than the best interest of children'.¹⁴ Many of the strategic directions and approved child protection mechanisms have deficiencies and some of them, including the monitoring of child abuse in institutional settings, are not monitored effectively.

In the Annual Report of the Ombudsman,¹⁵ the fact is highlighted that child poverty remains the reason of institutionalisation. This is considered to be a result of non-proportional coverage of the services. Restating the fact that community-based services have been improved, it indicates that 2 400 children remain institutionalised, even where the majority of these children have at least one parents. Among the negative issues mentioned in the report were child marriages and limited access to alternative services. Although the funds allocated to the improvement of children's lives as far as education, health care and legal protection are concerned remain limited, there still is a need for improving the institutional capacities of child protection bodies.

The PCA between the EU (EC) and Armenia, signed in 1999, mentions respect of human rights as part of the Agreement.¹⁶ It also envisages respect and promotion of human rights through political dialogue.¹⁷ Although the language of the Action Plans is neutral and not explicit, in comparison with some fields indicating certain measures of improvement, child protection, and generally the protection of the rights of the child, is mentioned in a broad formulation.¹⁸

12 *Ad Hoc* Public Report, Armenia: Status of Commitments under the Convention on the Rights of the Child and Its Optional Protocols, 2018, Yerevan 9-10, available at www.ombuds.am (last visited 15 February 2017).

13 *Ad Hoc* Public Report (n 12) 13. In 2018 to 2020 Medium-Term Public Expenditure Framework the fields will be reduced to 1,06 per cent for health and 1,85 per cent for education.

14 *Ad Hoc* Public Report 24.

15 Annual Communiqué on the Activities of the Human Rights Defender of the Republic of Armenia and the State of Protection of human rights and Freedoms during the Year 2017, Yerevan, 2018, available at <http://www.ombuds.am/resources/ombudsman/uploads/files/publications/b738f4eb767ab62bedef29f766fa9ea0.pdf> (last visited 15 February 2017).

16 European Communities 'Partnership and Cooperation Agreement between the European Communities and their Member States, of the one part, and the Republic of Armenia, of the other part', Official Journal of the European Communities L 239/3, 9.9.1999, art 2.

17 European Communities (n 16) art 5 para 3.

18 European Communities (n 16) Priority Area 3.

The only programme reported in 2018, entitled 'EU4Citizens', which focused on the support in human rights, was the organisation of National Assembly elections and the improvements of respect for fundamental rights.¹⁹

Another cornerstone in the EU cooperation with Armenia was put in place with the launch of the Comprehensive and Enhanced Partnership Agreement between the European Union and the Republic of Armenia (CEPA) in 2017. In the Agreement the general provisions and principles commit the parties to work on the improvement of the human rights situation in Armenia. In this regard the explicitly mentioned targets are 'the rights of persons belonging to minorities'. The only area where children were mentioned as a specific target group is respect of the development of judiciary cooperation in civil and commercial matters.²⁰

Armenia is the only country in the EaP to which a tailor-made agreement was offered, in the aftermath of its sudden membership to the Eurasian Economic Union. Considering the fact that the old government (the Republican Party) chose the Eurasian vector of external economy preference and that the new government has not yet positioned any changes in external policies, the EU remains loyal to its announced commitments within EaP. In this regard, Armenia stopped belonging to the 'outlier clause' category country. The discrepancy between the political dynamics in Armenia and the EU's reluctance of cooperation with the neighbours of this category, come to prove that the outlier clause does not support the EU's aspirations of becoming a global power. The human rights agenda for the EU and Armenia has not contributed much in the field of child protection. However, the CEPA agreement includes provisions that may inspire future changes.

4.2 Georgia

Georgia ratified CRC in 1994, and its two Optional Protocols in 2005 and 2010. Moreover, by ratifying the Vienna Convention on the Law of Treaties, Georgia undertook to give priority to international law over any conflicting national legislation. CRC principles have also been fully incorporated into national law.²¹ Although there is no comprehensive data on Georgian court decisions, studies show that courts have on occasion explicitly referred to the principle of the 'best interests of the child', as contained in the CRC.²²

Among the child protection documents, Georgia has a separate Law on Juvenile Justice Code. Moreover, in February 2019 the draft Code on the Rights of the Child was presented to the public to invite discussions on its content. The Law covers all the rights and freedoms of the child, describe the mechanisms of their protection and implementation, target the equity

19 Commission Implementing Decision of 26 November 2018 on annual programme in favour of the Republic of Armenia for 2018 (6) 2.

20 Comprehensive and Enhanced Partnership Agreement between the European Union and the Republic of Armenia in 2017, art 20.

21 Law of Georgia on International Treaties, art 6, available at https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=33442 (last visited 10 March 2019).

22 (CRIN), Access to Justice for Children: Georgia, January 2015, available at https://archive.crin.org/sites/default/files/georgia_access_to_justice_0.pdf (last visited 10 March 2019).

gaps in the realisation of their rights and strengthens the public mechanisms of accountability in realising the full protection of children.²³ This draft was adopted to address the state's low score on the 2016 Child Protection Index, with a ranking in the ninth position among nine countries (Child Rights International Network 2015). Currently Georgia has neither a coordination mechanism between central and local government for monitoring and assessing policy implementation, nor a national-level consultation mechanism to engage civil society or children directly in respect of the policy development and implementation (Child Pact, World Vision, Child Protection Index: Georgia, Measuring the Fulfilment of the Child's Right).²⁴ No parliamentary body has as yet been created to assess and solve child protection issues. However, the significant role of the human rights defender is mentioned. Among the positive results, Georgia is one of the front-runners in foster care, with almost 64 per cent of children separated from their families living with foster care families.²⁵

As determined by the Asian Development Bank, there are four major reasons of poverty in Georgia: 'lack of economic opportunity; isolation; insufficient skills, capabilities, and assets; income shocks due to health events or disasters' (Asian Development Bank, Poverty Analysis: Georgia).²⁶ Poverty has a predominantly rural character (with 25 per cent of the rural population being poor), and has increased since 2003.²⁷

Child poverty was reported to be one of the main issues since the war in Abkhazia and South Ossetia. After the deterioration of the Georgian economy in 2015 and 2016, the subsequent two years displayed significant progress. Although child poverty in the country is low, it has increased by 2 per cent between 2015 and 2017.²⁸ The welfare studies in Georgia show that children are more likely to be poorer than the general population or pensioners.²⁹

Apart from the successful implementation of the Partnership and Cooperation Agreement, Georgia was ahead of Ukraine in concluding the Association Agreement with the EU in June 2014. Apart from the general statements and commitments of Georgia for the betterment of democracy, the rule of law and human rights, the Agreement stipulates the enforcement of the rights of persons belonging to minorities among its priority areas.³⁰ The effective abolition of child labour,³¹ the

23 UNICEF Georgia The Draft Code on the Rights of the Child presented to the public in Georgia, available at <https://www.unicef.org/georgia/press-releases/draft-code-rights-child-presented-public-georgia> (last visited 10 March 2019).

24 Child Pact, World Vision, Child Protection Index: Georgia, Measuring the Fulfilment of the Child's Rights, available at <http://www.childpact.org/wp-content/uploads/2015/06/Child-Protection-Index-Georgia.pdf> (last visited 10 March 2019).

25 Child Pact, World Vision, Child Protection Index (n 24) 15.

26 Asian Development Bank, Poverty Analysis: Georgia, available at <https://www.adb.org/sites/default/files/linked-documents/cps-geo-2014-2018-pa.pdf> (last visited 10 March 2019).

27 As above.

28 'The share of households and the population below the relative poverty line increased from 20,7% to 22,5% and from 23,1% to 31,6%. The percentage of children living in poor households increased from 26,8% to 31,6%. UNICEF Analysis of the Georgia Welfare Mentoring Survey Data, 2017, available at <https://www.unicef.org/georgia/reports/wellbeing-children-and-their-families-georgia-fifth-stage-2017> (last visited 10 February 2019).

29 UNICEF (n 28) 134.

modernisation of education³² and judicial cooperation for protection of children³³ are inseparable parts of the Agreement. Some of these areas were also stipulated in the Action Plan of Georgia, including the commitment to reduce child poverty through social security reforms and full implementation of international obligations related to child labour and abduction.

Moreover, the Association Agenda specified a special guidance in improving child protection in the country. In particular, the Agenda urges Georgia to address children's poverty, continue juvenile justice reforms, include child rights into the National Human Rights Strategy and Action Plan, as well as to provide adequate resources for the Public Defender for undertaking ombudsmen work for children and focus measures to protect children from all sorts of violence.

Human rights were one of the pivotal points mentioned in the Association Agreement Report of January 2019. Georgia was observed to have made significant progress in upgrading the national legislation with regard to the violence against women, fighting torture, inhuman and degrading treatments in detention facilities, and in country mechanisms related to the effective human rights protection in the breakaway region of Abkhazia and South Ossetia and bordering communities. The EU remains concerned about the infant mortality rate, which is significantly higher than in Europe. It also highlighted the high rates of children who live in poor families, unregulated child protection mechanisms, and the slow-down in deinstitutionalization processes (Association agreement between EU and Georgia p 9).³⁴

As reported, human rights protection in Georgia was funded by EU MFA with the first instalment of €20 million (€15 million in loans and €5 million in grants) by the end of 2018 and a second earmarked for 2019.³⁵ The financial contributions of the EU for the improvement of human rights are also directed from the European Instrument for Democracy and Human Rights, as part of the European Neighbourhood Instrument. Georgia remains the only state among the EaP countries that has signed the DCFTA and was the first to benefit from the visa liberalisation decision of the EU. However, despite the fact that so far Georgia has been most responsive to the EU's agenda, it remains in the 'muddling through' phase. The EU has no further mechanisms of appreciating Georgia's progress in benchmarked areas, whereas the 'everything but membership' clause is still applicable for EaP countries.

Compared to Armenia and Ukraine, the cooperation between the EU and Georgia has gone further. The EU's contribution in human right reforms in the country is significant. However, the analysis of the country's human rights and child protection reforms are motivated more by

30 Association Agreement between EU and Georgia, art 3, Aims of Political Dialogue (h).

31 Association Agreement (n 30) art 229 para 2(c).

32 Association Agreement (n 30) art 359(b).

33 Association Agreement (n 30) art 21.

34 Association Agreement (n 30) 6.

35 EEAS Association Agreement Report 2019, Georgia, available at https://eeas.europa.eu/sites/eeas/files/2019_association_implementation_report_georgia.pdf (last visited 10 March 2019).

imperatives for domestic implementation than the EU's commitment to human rights and child protection.

4.3 Ukraine

Ukraine ratified the CRC in 1991. The CRC is incorporated into national law, is directly enforceable, and has a status superior to national law. Article 9 of the Constitution of Ukraine provides for the integration of an array of treaties into national legislation as mandated by the Parliament of Ukraine.³⁶ Among the key domestic legislation and regulations are the Civil Code and Family Code of Ukraine (which both entered into force in 2004, thereby implementing the conclusions and recommendation of the UNCRC), the Laws of Ukraine on Provision of Organisational and Legal Conditions for Social Protection of Orphans and Children without Parental Care, and on the Main Principles of Social Protection of Homeless Persons and Street Children adopted in 2005.

The judicial system of Ukraine also provides that a child of any age can report a criminal offence to an investigator or a prosecutor. Children are also allowed to appeal to the Human Rights Commission of the Ukrainian Parliament and request judicial review by the Constitutional Court (Child Rights International Network 2014). However, there are no family or children's courts in Ukraine, and disputes are handled by the local courts of general jurisdiction.

As of September 2015, there were 99 915 children living in 663 institutions in Ukraine. The data does not include the number of institutions and children in areas over which Russia and Ukraine have ongoing disputes (Hope and Homes for Children 2015). There are 33 types of institutions which are managed by three different public authorities: 38 infant homes that function under the Ministry of Health; 50 children's care homes that are managed by the Ministry of Social Policy; and 575 residential facilities of different types that are supervised by the Ministry of Education and Science of Ukraine (Hope and Homes for Children 2015: 9). Of these institutions, 45 per cent were established in the period from 1951 to 1970. Most of the buildings are located in remote and inaccessible parts of cities.

The National Human Rights Strategy of Ukraine of 2015-2020 highlights child protection as one of its strategic areas. The goals of the strategic area are 'to create a favourable environment for the upbringing, education and development of children and set up an efficient system of the rights of the child' and 'to improve state mechanisms of observing the right of the child'.³⁷ Highlights within the defined Action Plan are the enhancement of child protection systems (including the juvenile justice system, provision of temporary settlements); of institutions; of the living conditions of children in the family and special facilities; and to ensure the minimal standards of security and well-being of the child.³⁸

36 The list includes the Optional Protocols to CRC, conventions of the Council of Europe and Hague Conferences, cooperation agreements with CIS member states and several others.

37 Decree of the President of Ukraine 501/2015 on Approval of the National Human Rights Strategy of Ukraine, August 2015 14.

38 As above.

The priority areas of the Ukrainian child protection policies have changed after the war with Russia, with the focus falling on the social rights of children in conflict situations. According to the available resources most of the children from the contact line regions lack access to education, availability of the health facilities and there are poor mechanisms for monitoring the management of child protection issues at grassroots level. Because of the high militarisation along the Eastern Ukrainian borders, children are being engaged in the military activities, with girls above the age of 14 years often engaged in sexual relations with the military, leading to child pregnancy and a high incidence in HIV infection.

After the erupted war in the Eastern Ukraine, the human rights monitoring missions monitored human rights violations in these regions. The periodic reports state that there are massive human rights violations in conflict-affected areas, emanating in civilian casualties and economic and social deprivation. According to the Office of the United Nations High Commissioner for Human Rights the human rights violations are on-going in the conflicting areas.³⁹ The report points out the violations of international humanitarian law, limitations of freedoms of opinion and expression, peaceful assembly and religion/belief. According to the findings of the report of 2018, 435 individuals were deported and forcibly removed from Crimea, among them 231 Ukrainian nationals. These people were considered foreigners under Russian Federation law.⁴⁰ The entry to the peninsula is limited to journalists. No specific cases concerning particularly children's rights in these areas are mentioned in the report. However, the civilians bearing the consequences of war have limited access to fair trials, the justice system and basic needs such as water facilities.⁴¹ The evolved situation speaks loudly about the insecure environment that undermines the best interests of children. Children and their families continue to experience significant disruption to their daily lives after more than four years of regular conflict and clashes between government-controlled areas and non-government controlled areas.

In 2017 UNICEF Ukraine initiated Country Programme 2018-2022. The main areas of importance are the adolescent mobilisation, their participation in decision making and the attention to age-responsive healthcare services.⁴² Social protection was included in the EU's Single Support Framework for Ukraine 2018-2020 on assisting the social protection 'for conflict affected communities, internally displaced persons in the context of the ongoing decentralisation reform'.⁴³

The Association Agreement between the EU and Ukraine was signed in 2014. Among the aims of the agreement it is mentioned 'to enhance cooperation in the field of justice, freedom and security with the aim of reinforcing the rule of law and respect for human rights and fundamental

39 Office of the United Nations High Commissioner for Human Rights, Report on the human rights situation in Ukraine 16 November 2018 to 15 February 2019, available at <https://www.ohchr.org/Documents/Countries/UA/ReportUkraine16Nov2018-15Feb2019.pdf> (last visited 10 April 2019).

40 OHCHR (n 40)(d)30.

41 OHCHR (n 40)(c)34.

42 UNICEF Annual Report 2017, Ukraine, available at https://www.unicef.org/about/annualreport/files/Ukraine_2017_COAR.pdf (last visited 10 February 2019).

43 UNICEF (n 43) 8.

freedoms'.⁴⁴ Among the narrower human rights cooperation directions, the main areas defined are the cooperation on migration, asylum and border management, cooperation in fighting terrorism, trafficking protection of personal data and other reforms concerning the betterment of the rule of law and justice system. The 2018 Report on Implementation of the Association Agreement between Ukraine and the EU assessed the implementation of the scheduled activities under the Agreement as having been performed at 52 per cent.⁴⁵

In 2017 the EU Instrument for Democracy and Human Rights allocated approximately €25 million for five recurring 'human rights lots' of the period 2014-2017. These included the human rights of indigenous people, extra-judicial killings, labour rights and slavery, the rights of persons with disabilities and support to freedom of religion and belief. The announced priority areas under the 2018 call were human rights protection agencies. The three key areas announced were '(i) to enable human rights defenders at risk (individuals, groups and organisations) to carry out their work; (ii) to enhance temporary relocation and shelter capacities; and (iii) to strengthen the coordination and synergy with other actors'.⁴⁶

The EU's 2017-2018 agenda to promote and fulfil human rights is quite extensive. In 2017 a two-year project to support the Ukrainian administration for setting up an early intervention and rehabilitation for children with disabilities was launched, allocating €1.3 million. A significant number of projects have been directed to the war-affected areas and internally displaced people. Among these are projects of capacity building for human rights defenders in Ukraine and Crimea (€300k, 2018); supporting recovery and Sustainable Solutions for Internally Displaced Persons and Conflict-Affected Population in Ukraine (with IOM, completed in June 2018, €4 million); strengthening the capacities of CSOs and other services for improved integration of internally displaced children, completed by February 2018, €280k) and several others.⁴⁷ The EU's allocation of funds and support to a human rights sector demonstrates the political feel, competence and available resources of the EU to intervene in the EaP regions in cases of demand and cooperation with the CSOs.

Ukraine plays a pivotal role in the EU's external policy and relations with Russia. However, the slow pace of reforms and of the fight against corrupt political systems, and low indicators of human rights protection, give more incentive for the EU to further liberalise visa regimes and expand economic partnerships. In this regard, Ukraine is an example of an 'unconditional love' clause.

44 Association Agreement between the European Union and its member states, of the one part, and Ukraine, of the other part, art 1, Objectives, 2(e) 2014.

45 Association Agreement Implementation Report 2018, available at <http://www.3dcftas.eu/system/tdfs/association-agreement-implementation-report-2018-english.pdf?file=1&type=node&id=552> (last visited 10 March 2019).

46 European Instrument for Democracy and Human Rights (EIDHR), Reviewing the European Union Human Rights Defenders Mechanism, Guidelines for grant applicants, Restricted Call for Proposals 2018.

47 EU delegation in Ukraine, Projects, available at https://eeas.europa.eu/delegations/ukraine/area/projects_en?page=3 (last visited 10 March 2019).

5 Conclusion

The selected achievements and perplexing issues arising during 2018 in three EaP countries demonstrate that the region is in need of developing better child protection policies. These countries should strive for the eradication of poverty among children and their families, to minimise the negative consequences of conflicts on the enjoyment of childhood, and to strengthen domestic child protection mechanisms. Since the establishment of the ENP and the launch of the EaP, the EU positioned itself to be another guarantor of human rights promotion, protection and fulfilment in Armenia, Georgia and Ukraine. Despite the enthusiasm and manifold cooperative endeavours within the EU, human rights and child protection remains left behind. The demonstrated backslides from the child rights agenda should be tackled within extensive investment. Above all, the cooperation of international and regional organisations should consolidate efforts to combat child rights violations in each of the countries.

References

- Ad Hoc* Public Report, Armenia: Status of Commitments under the Convention on the Rights of the Child and Its Optional Protocols, 2018, Yerevan 9-10, available at www.ombuds.am (last visited 10 March 2019)
- Annual Communiqué on the Activities of the Human Rights Defender of the Republic of Armenia and the State of Protection of human rights and Freedoms during the Year 2017, Yerevan, 2018, available at <http://www.ombuds.am/resources/ombudsman/uploads/files/publications/b738f4eb767ab62bedef29f766fa9ea0.pdf> (last visited 10 March 2019)
- Armenian Child Protection Network, Child Protection Index Armenia 2016, available at <http://2016.childprotectionindex.org/country/armenia> (last visited 15 February 2017)
- Asian Development Bank, Poverty Analysis: Georgia, available at <https://www.adb.org/sites/default/files/linked-documents/cps-geo-2014-2018-pa.pdf> (last visited 10 March 2019)
- Association Agreement between EU and Georgia, 2015
- Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part, article 1, Objectives, 2(e) 2014
- Association Agreement Implementation Report 2018, available at <http://www.3dcftas.eu/system/tdf/association-agreement-implementation-report-2018-english.pdf?file=1&type=node&id=552> (last visited 10 March 2019)
- Child Pact, World Vision, Child Protection Index, Georgia, Measuring Government's Efforts to protect Boys and Girls Georgia, 2016, available at <https://www.dropbox.com/s/e626u7qs08zm2os/CPI-Georgia.pdf> (last visited 10 March 2019)
- Child Pact, World Vision, Child Protection Index: Georgia, Measuring the Fulfilment of the Child's Right, available at <http://www.childpact.org/wp-content/uploads/2015/06/Child-Protection-Index-Georgia.pdf> (last visited 10 March 2019)

- Child Rights International Network (CRIN), Access to Justice for Children: Georgia, January 2015, available at https://archive.crin.org/sites/default/files/georgia_access_to_justice_0.pdf (last visited 10 March 2019)
- Child Rights International Network, Ukraine: Access to Justice for Children, April 2014, available at <https://home.crin.org/> (last visited 10 March 2019)
- CoE, Council of Europe Strategy for the Rights of the Child (2016-2021), Sofia, April 2016, available at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8> (last visited 27 March 2017)
- Commission Implementing Decision of 26 November 2018 on annual programme in favour of the Republic of Armenia for 2018 (6)
- Comprehensive and Enhanced Partnership Agreement between the European Union and the Republic of Armenia in 2017, article 20
- Council of Europe Policy Guidelines on Integrated National Strategies for the Protection of Children from Violence, Strasbourg, November 2009, available at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046d3a0> (last visited 17 March 2017)
- Council of Europe, European Social Charter (Revised), Strasbourg, 3V.1996, European Treaty Series 163, Strasbourg, 1996
- Council of Europe, European Court of Human Rights, European Convention on Human Rights, Rome, 1950 30, available at http://www.echr.coe.int/Documents/Convention_ENG.pdf (last visited 8 February 2017)
- Craig P & De Burca G (2003) *EU law, text, cases and materials* Oxford: Clarendon Press Ltd
- Decree of the President of Ukraine 501/2015 on Approval of the National Human Rights Strategy of Ukraine, August 2015
- EEAS Association Agreement Report 2019, Georgia, available at https://eeas.europa.eu/sites/eeas/files/2019_association_implementation_report_georgia.pdf (last visited 10 March 2019)
- EU delegation in Ukraine, Projects, available at https://eeas.europa.eu/delegations/ukraine/area/projects_en?page=3 (last visited 10 March 2019)
- EU Delegation to the United Nations-New York, EU Statement United Nations 3rd Committee: Rights of Children, 13 October 2016, New York, available at <http://eu-un.europa.eu/eu-statement-united-nations-3rd-committee-rights-children/> (last visited 8 February 2017)
- EU Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Official Journal of the European Union, 2016/C 202, 7.6.2016, article 6(1) TEU
- EU Guidelines for the Promotion and Protection of the Rights of the Child (2017), Key Messages 3, available at https://eeas.europa.eu/sites/eeas/files/key_messages_-_eu_guidelines_on_children.pdf (last visited 10 March 2017)
- EURlex, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A new repose to a changing Neighbourhood/*COM/2011/0303 final*/, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011DC0303> (last visited 1 April 2017)
- European Commission Implementing Decision of 29 October 2014 on the Annual Action Programme 2014 in favour of the Republic of Armenia to be financed from the general budget of the European Union, Brussels, 29 October 2014
- European Commission COM (2012), 130 final, 2012/0064 (APP), Brussels 21 March 2012

- European Communities Partnership and Cooperation Agreement between the European Communities and their Member States, of the one part, and the Republic of Armenia, of the other part, Official Journal of the European Communities L 239/3, 9.9.1999
- European Instrument for Democracy and Human Rights (EIDHR), Reviewing the European Union Human Rights Defenders Mechanism, Guidelines for grant applicants, Restricted Call for Proposals 2018
- European Union Charter of Fundamental Rights of the European Union, Official Journal of the European Union, 2016/C 202/02, 7.6.2016
- Government of Republic of Armenia, Decree 1273 of the Government of the RA on Amendments in Decree 1694 of the Government of RA, Yerevan, November 2014
- Government of Republic of Armenia, Decree 1694 of 27 December 2012 on Protection of the Child Rights Strategic Plan of 2013-2016 and Approval of the Agenda of 2013-2016 Strategic Plan and Recognising the of Decree 1745 of December 18 Invalid, Yerevan 2012
- Government of Republic of Armenia, Decree 1745 of 18 December 2003 on Adopting Child Protection National Plan of 2004-2015, Yerevan, 2003
- Government of Republic of Armenia, Draft of the RA Decree on Child Protection Strategy of 2017-2021 *Ad Hoc* Action Plan of Child Protection Strategy 2017-2021, Chapter VII, available at <http://www.mlsa.am/forum/forum.php?sec=conference> (last visited 30 March 2017)
- Hope and Homes for Children 'The Illusion of Protection' an analytical report based on the findings of a comprehensive study of the child protection System in Ukraine, 2015, available at https://www.openingdoors.eu/wp-content/uploads/2017/12/The-illusion-of-protection_eng.pdf (last visited 30 March 2017)
- ILO C182 Worst Forms of Child Labour Convention, 1999 (182), Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour, Geneva 1999
- Kombe J-FA 'Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights, Directorate-General of Human Rights' (2007) *Human Rights Handbooks* Belgium: Council of Europe
- Law of Georgia on International Treaties, article 6, available at https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=33442 (last visited 10 March 2019)
- Law of the Republic of Armenia on Social Support, adopted 17 December 2014, Chapter 7 System of Social Support Services, Social Cooperation and Local Social Projects, Yerevan, 2014
- National Assembly of Republic of Armenia The Law of the Republic of Armenia on the Child's Rights, 29 May 1996, non-official translation, available at <http://www.ombuds.am/resources/ombudsman/uploads/files/agreements/2d25331b2ad440a56d9e450a307813f3.pdf> (last visited 3 March 2017)
- Office of the United Nations High Commissioner for Human Rights, Report on the Human Rights Situation in Ukraine 16 November 2018 to 15 February 2019, available at https://www.ohchr.org/Documents/Countries/UA/Report_Ukraine16Nov2018-15Feb2019.pdf (last visited 10 April 2019)
- Republic of Armenia, Criminal Code of the Republic of Armenia, non-official translation, Yerevan, 18 April 2003

- State Statistics Service of Republic of Armenia, Child Labour State Study 2015, available at <http://www.armstat.am/file/doc/99499668.pdf> (last visited 2 April 2017)
- UN GA, Preamble of Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, adopted and opened for signature, ratification and accession by General Assembly Resolution A/RES/54/263 of 25 May 2000 entered into force on 18 January 2002, New York, 2002
- UN General Assembly, Resolution 70/1, Transforming Our World: The 2030 Agenda for Sustainable Development, 25 September 2015
- UN Treaty Series, International Covenant on Civil and Political Rights, New York 1976
- UN Addis Ababa Action Agenda of the Third International Conference on Financing for Development (Addis Ababa Action Agenda), New York 2015, available at <https://sustainabledevelopment.un.org/post2015/transformingourworld> (last visited 28 February 2017)
- UN Convention on the Elimination of All Forms of Discrimination against Women, New York 1981
- UN Convention on the Rights of the Child, General Comment 5, General Measures of Implementation of the Convention on the Rights of the Child (articles 4, 42 and 44) CRC/GC/2003/5, 27 November 2003
- UN Convention on the Rights of the Child, New York 1989
- UNICEF Annual Report 2017, Ukraine, available at https://www.unicef.org/about/annualreport/files/Ukraine_2017_COAR.pdf (last visited 10 February 2019)
- UNICEF Georgia, The Draft Code on the Rights of the Child presented to the public in Georgia, available at <https://www.unicef.org/georgia/press-releases/draft-code-rights-child-presented-public-georgia> (last visited 10 March 2019)
- UNICEF Analysis of the Georgia Welfare Mentoring Survey Data, 2017, available at <https://www.unicef.org/georgia/reports/wellbeing-children-and-their-families-georgia-fifth-stage-2017> (last visited 10 February 2019)

Recent developments in sub-Saharan Africa during 2018

Ashwanee Budoo, Adem Abebe,***

*Stephen Buabeng-Baidoo*** and Henok Ashagrey*****

Abstract: This article highlights selected developments in democracy and human rights in Africa during 2018. While highlighting the progress that Africa has made in relation to democracy in countries such as Ethiopia, Angola, South Africa and Sierra Leone, it demonstrates how the situations in Uganda, Cameroon and Togo continued to be an attack on democracy. It also explains how, despite the lack of focus on democracy in the African Continental Free Trade Agreement, this Agreement can lead to more democratic governance with respect for the rule of law in African countries. It then focuses on developments within the African Commission on Human and Peoples' Rights, the African Court on Human and Peoples' Rights and the African Committee of Experts on the Rights and Welfare of the Child. In 2018 these judicial and quasi-judicial human rights institutions have handed down decisions or adopted soft laws with a view to better protecting human rights across the continent.

Key words: democracy; human rights; African Commission on Human and Peoples' Rights; African Committee of Experts on the Rights and Welfare of the Child; African Court on Human and Peoples' Rights; communications

1 Introduction

This article highlights selected developments regarding democracy and human rights in Africa in the year 2018. It first analyses accounts of progress, recession and stagnation concerning democracy at the African level. Second, it assesses developments within the judicial and human rights institutions of the African Union (AU), including the African Commission on Human and Peoples' Rights (African Commission), the African Court on Human and Peoples' Rights (African Court) and the African Committee of Experts on the Rights and Welfare of the Child (African Children's Committee). The final part concludes the article.

* LLD; Programme Manager, Centre for Human Rights, University of Pretoria; ashwanee.budoo@up.ac.za

** LLD; Programme Officer, Constitution Building Programme, International IDEA; Extraordinary Lecturer, Centre for Human Rights, University of Pretoria; adem.abeb@gmail.com

*** LLM; Legal Assistant, Secretariat of the African Commission on Human and Peoples' Rights; stephenbbaidoo@yahoo.com

**** LLM; Lecturer of Law, Dilla University; hendulsa@gmail.com

2 Democracy in Africa in 2018: Accounts of progress, recession and stagnation

On a continent comprising 55 countries a single, overarching story is unlikely to make much sense on any theme, much less on the contested concept and practice of democracy. In 2018, as before, the tale of democracy was mixed, with some countries on the continent witnessing gains, others recession and many stagnating. Freedom House (2019: 12) captures the diverse dynamics aptly, noting both 'historic openings' and 'creeping restrictions'. According to the rankings for sub-Saharan Africa, 18 per cent of the population live in countries that are categorised as 'free', 43 per cent in 'partly free' and 39 per cent in 'not free' countries.

This part provides a snippet of the most notable accounts of democratic progress and set-back on the continent during 2018. While the focus is on countries with significant movements in the democracy spectrum, it is also important to mention developments in some countries with critical implications. In particular, in May 2018 Mozambique amended its Constitution to implement a token of decentralisation of political powers with a view to responding to regionalised political preferences and to enable the end of intractable, long-running low-level conflict (Kössler 2018). These changes could enhance political inclusivity, participation and accountability. Tunisia's local elections in May 2018 returned almost half female local council members and more than 37 per cent youth members, thanks to a new election law (Mekki 2018). In July 2018 Zimbabwe for the first time in four decades held elections without long-time leader Robert Mugabe (Feldstein 2018). Burundian President Pierre Nkurunziza has pledged to step down at the end of his current term, guaranteeing a peaceful change of faces at the top (News24 2018), despite the adoption of a new Constitution that potentially allows him to again run for office. In contrast, in May 2018 President Azali Assoumani of Comoros orchestrated a constitutional amendment allowing him to run again and concentrating power in the national government and the presidency (Parmentier 2018). He was re-elected in a controversial election in July 2019 that saw leading opposition figures arrested. While the excitement often is focused on the obvious examples, these and similar developments contribute to or undermine the reach, inclusivity and consolidation of democracy, and therefore deserve continued mention.

2.1 Hopes for democratic progress

The year 2018 witnessed notable high-profile changes of leadership in many corners of the continent, from South Africa to Ethiopia and from Angola to Sierra Leone. According to Freedom House's 2018 Freedom in the World report, three of the six countries that recorded most progress in the world are from Africa (Angola, Ethiopia and The Gambia). These changes of faces in the highest political offices have sparked hope and momentum for democratic gains.

Perhaps the most dramatic account of political transition in 2018 occurred in Ethiopia. Following months of protests and intra-party power struggle, Hailemariam Desalegn resigned as Prime Minister in February 2018, and in April 2018 Parliament confirmed Abiy Ahmed as the replacement (TRT World 2018). The new Prime Minister ordered the release of political prisoners, recognised opposition groups as legitimate

political contenders, invited exiled politicians to the country and initiated a reform drive that has captured continental and global eyes. Abiy also appointed women to half of the cabinet positions, and saw the appointment of the first women president, chief justice and head of the National Electoral Board. Crucially, an advisory council was established under the office of the Attorney-General to reform laws critical to democratic dispensation, including the election law and the law establishing the Electoral Board, as well as laws governing civil society organisations (CSOs), the media and terrorism. The much-criticised CSO law has been replaced and a new law regulating the Electoral Board has been adopted. New election and media laws are also in the pipeline and are expected to be adopted before the next elections, planned for May 2020. In the meantime, new private printing and broadcasting media have mushroomed and prominent exiled media houses have established offices in the country. The Committee to Protect Journalists announced that at the end of 2018 Ethiopia had no journalists in prison, the first since 2004 (Dahir 2018). However, the ongoing transition has not been without hiccups and its success is far from certain. The loosening of government control has led to serious instances of breakdown of law and order, mob justice, inter-ethnic competition and conflict and large-scale internal displacement. This situation has led to the postponement of the national census and has prompted calls for the delay of the May 2020 elections, with unpredictable consequences for the country's democratic trajectory. The government of Abiy Ahmed must find ways of taming unprecedented levels of ethnic nationalism and mobilisation and re-establish its monopoly of violence to provide a stable basis for democratic transition.

Another country that has seen an unprecedented change of leadership is Angola. After 38 years in power, President Dos Santos stepped down in August 2017 and, in September 2018, resigned as head of the ruling party, People's Movement for the Liberation of Angola (MPLA). After taking power under largely low expectations, his replacement, President Joao Lourenco, has taken significant measures most notably against corruption and the dismantling of the extensive economic empire of the family of the former President, as well as in enhancing the level of judicial independence (Powell 2018). Progress in the overall democratic trajectory would require measures to ease systematic pressure and disadvantages on opposition groups, CSOs and the media.

While Ethiopia and Angola's status in Freedom House's democracy index remains 'not free', the two countries received specific mention as among the most improved in 2018.

After years of scandals involving corruption and mismanagement, President Jacob Zuma of South Africa was forced to resign from his position in February 2018. The ruling party, the African National Congress (ANC), orchestrated the transition, which (re)confirmed the capacity of constitutional and political institutions to manage the contested but largely orderly transition. Zuma's replacement, Cyril Ramaphosa, who has been beleaguered by a controversial political past, notably in connection with the killing of miners in Marikana in 2012, nevertheless is seen as a reformer (Jeffery 2019). In the April 2019 elections the ANC, with Ramaphosa as the flag-bearer, won a parliamentary majority. Parliament subsequently confirmed Ramaphosa as President (Al Jazeera 2019). An advance in South Africa's democratic

credentials would require significant introspection and the dismantling of the political culture, institutional environment and impunity that has allowed and enabled the thriving of high-level corruption.

While the transitions in the above three countries occurred within the same ruling parties, Sierra Leone witnessed the ascendance into power of the main opposition party (Al Jazeera 2018). President Ernest Bai Koroma was barred from running for President due to term limits. Despite reports of attempts to remove term limits, Koroma stepped down as constitutionally required. His party therefore had to nominate a replacement to run for the March 2018 presidential election. Samura Kamara was nominated as the flag-bearer of the ruling party but lost to the main opposition candidate Julius Maada Bio in a run-off election. The Sierra Leonean story affirms the importance of term limits in enhancing the chances of democratic transition and consolidation. Evidence suggests that the chances of victory of opposition groups are higher in cases where the incumbent President does not run for election (Posner & Young 2018). Term limits help to break the 'incumbency advantage' and provide opportunities for relatively free and fair elections and democratic transitions.

2.2 Democratic stagnation and recession

The signs of progress in some African countries have been accompanied by stagnation and recession in others, especially those under long-term incumbents.

Hopes for democratic transition in Uganda have been dashed following a constitutional amendment that removed age limits on presidential candidates to allow long-time incumbent President Yoweri Museveni to run unencumbered (Ssemogerere 2018). Museveni has ruled Uganda since 1986. In 2005 he orchestrated the removal of presidential term limits to enable him to run again. The latest amendment, which the courts have found compatible with the Constitution (Biryabarema 2019), implies that Museveni is likely to lead the country for the foreseeable future. The ease with which Museveni has deployed constitutional amendment procedures to undermine limits on the presidency demonstrates the need for stronger protection of certain vulnerable constitutional provisions (Abebe 2019). In combination with attacks on opposition hopefuls, notably musician-turned-politician Bob Wine, and restrictions on the media and CSOs, Uganda has effectively cemented its authoritarian reputation, as evidenced in the transition from 'partly free' to 'not free' in the Freedom House categorisation.

Another long-time ruler, Cameroon's Paul Biya, was declared the winner of the presidential elections in October 2018 (De Marie Heungoup 2019). The 86 year-old President is now serving his seventh term and has ruled the country since 1982. Despite his old age, there are no public talks of succession and the consequences of a sudden passing of the ageing President remain unpredictable. Biya's regime has successfully undermined opposition groups and independent voices, undermining any hopes for a democratic future. These challenges to democratic progress have exacerbated tensions arising from demands for self-determination from Cameroon's Anglophone regions. The inability of the political process and state institutions to resolve the tension has led to an intractable armed conflict and a brutal state crackdown on Anglophone regions. Cameroon's

long-term stability requires significant willingness and efforts to address the related twin problems of democratisation and a level of autonomy and inclusion for all groups.

Hopes for democratic progress have also faded in Togo, which since August 2017 has seen significant popular protests. The main protest demand has been an end to the rule of the Gnassingbé family, which has governed the country for decades. President Faure Gnassingbé took power following the passing of his father, the long-time leader Gnassingbé Eyadéma. Opposition groups have been seeking the reinstatement of the 1992 Constitution which imposed two term limits on the presidency and the stepping down of Faure Gnassingbé, as well as reforms to several critical institutions, including the electoral commission and constitutional court, as a precondition for free and fair elections (Bado 2019). Nevertheless, the Togolese government resisted these reforms and instead proposed constitutional reforms that could keep Faure Gnassingbé for at least two more terms. An initial attempt to enact these amendments failed in September 2017 as the ruling party could not garner the necessary parliamentary vote to avoid a referendum on the proposals. While the government indicated that a referendum would be held, this did not materialise. Following the mediation efforts of the Economic Community of West African States (ECOWAS), plans were made for institutional reforms and delayed elections. However, the necessary constitutional and institutional reforms were not enacted and opposition groups boycotted legislative elections organised in December 2018. Under pressure from ECOWAS, the government postponed the planned referendum on constitutional amendments. Nevertheless, the opposition boycott allowed the ruling party to achieve a landslide victory in the December elections giving it the required numbers to amend the Constitution without the need for a referendum. Indeed, in May 2019 Parliament overwhelmingly approved the amendments (*Daily Mail* 2019). Under the amendments Faure Gnassingbé can run for two more terms. The amendments also give full immunity to all ex-presidents and limit the term of parliamentarians to two six-year terms. The changes have provided a veneer of constitutional legitimacy and consolidated Togo's authoritarian regime.

2.3 The African Continental Free Trade Agreement and prospects for democratisation

Perhaps the most notable progress at the African level in 2018 was the adoption of the African Continental Free Trade Agreement (AfCFTA). Following the deposit of the required number of 22 ratifications, the Agreement entered into force in May 2019. As at June 2019, 24 countries have ratified and 52 of the 55 African countries have signed the Agreement. While the principal focus of the Agreement is the facilitation of trade in goods and services, it is likely to have implications for the rule of law, democracy (Fagbayibo 2019) and anti-corruption (Iheukwumere 2019) measures. Despite the lack of explicit reference to adherence to democratic norms in the Agreement, the successful implementation of cross-border trade requires confidence in the legal systems of each country. The existence of rule of law and anti-corruption measures are necessary for the equal treatment of businesses from across the continent. In the long term, rule of law measures could facilitate the conditions for democratic consolidation. Accordingly, the potential implications of the implementation of the Agreement to democratic consolidation requires

further engagement among policy makers, academics and research institutions.

3 Judicial and human rights institutions at the African Union level

The African Union (AU) has three judicial and human rights institutions, namely, the African Court, the African Commission and the African Children's Committee. This part elaborates on selected developments within each institution during 2018.

3.1 African Commission on Human and Peoples' Rights

Following the declaration of the AU Assembly in June 2016 regarding 2017-2026 as the Human and Peoples' Rights Decade in Africa, the period under review has seen a renewed commitment by a number of states towards fulfilling their obligations under the African Charter. The various measures undertaken by member states are due in part to the active role played by the African Commission as the premier organ in the promotion and protection of human rights in Africa. However, backsliding by several states and the ensuing rise of attacks on the Commission's independence underscore the still persistent gaps in its legal and administrative structure and its tenuous footing within the broader AU framework.

For the specific period under review, several crucial developments were identified as relating to the work of the African Commission. In its biannual Activity Reports for 2018, namely, the 44th and 45th Activity Reports, the African Commission highlighted various positive and negative developments concerning human rights in Africa. Specific areas of focus in this respect concern the ratification or lack thereof of international instruments by member states to the African Charter, the adoption of national laws as well as general state conduct. Additionally, the Commission often lists communications considered during these periods and publishes the contents of those decided on the merits or otherwise finalised.

As relates to its protective mandate, specifically the consideration of communications/complaints, during the period under review the African Commission was seized of 41 communications, issuing provisional measures in seven; declared around nine communications admissible and two inadmissible for non-exhaustion of domestic remedies, among other factors; and decided two communications on the merits.

Only one of the two communications decided on the merits, *Kwoyelo Thomas v Uganda*, was publicly available. The complainants alleged therein that the victim (Thomas Kwoyelo) was a child soldier, abducted by the Lord's Resistance Army (LRA) in 1987 in Northern Uganda. The complainants further alleged that in March 2009 the victim was shot and severely wounded on the battlefield in the Democratic Republic of the Congo (DRC). The victim was also allegedly abducted from a hospital while recovering from his injuries and held at a private residence in Uganda, where he was subjected to torture and inhumane treatment for three months, and denied access to legal representation and next of kin. In June 2009 and August 2010 the victim was charged with several offences under the Ugandan Penal Code and the Ugandan Geneva Conventions Act

of 1964 respectively. Consequently, the victim applied for amnesty under Uganda's 2000 Amnesty Act. The Ugandan Amnesty Commission declared that the victim was eligible for amnesty but Uganda's Director of Public Prosecutions (DPP) refused to issue an amnesty certificate. The matter was brought to the attention of the Ugandan Constitutional Court, which decided in favour of the victim declaring that he qualified for amnesty and called for the cessation of the trial against the victim.

In response, the Ugandan government filed two applications with the Supreme Court seeking an interim order for the stay of execution of the consequential orders arising from the Constitutional Court's decision. Notwithstanding this, the International Criminal Division of the High Court of Uganda (ICD) proceeded to discontinue the victim's trial but Uganda refused to release the victim from detention. The High Court thereafter issued an order of *mandamus* to compel the Chairperson of the Amnesty Commission and the DPP to grant amnesty to the victim, to no avail. On 30 March 2012, the Supreme Court of Uganda stayed the execution of all consequential orders arising from the decision of the Constitutional Court. The complainants argued that the said decision of the Supreme Court had been adopted without reason and that the lack of quorum led to delays in finalising the appeal, thereby prolonging the victim's indefinite detention. Accordingly, the complainants alleged violations of the rights to equal protection before the law, non-discrimination, liberty and security of the person, as well as the right to be protected from torture, cruel, inhumane and degrading treatment as guaranteed in articles 2, 3, 4, 5, 6, 7(1)(a), (b), (d), 16 and 26 of the African Charter.

In its analysis, the African Commission observed that the victim had been captured while in active combat, during a non-international armed conflict, and thus the African Charter and the rules of international humanitarian law (IHL) would have concurrent application in the matter. The African Commission reasoned that in such instances it would only find violations on the African Charter but that the rules of IHL would serve as the standard for assessing the alleged violations. On the alleged violation of article 3, the African Commission observed that the victim was the only defendant before the Ugandan Amnesty Commission whose application had been rejected even though the amnesty requests of 24 000 other applicants had been granted. Additionally, the African Commission observed that Uganda's Amnesty Act provided blanket amnesty for those who 'renounced rebellion' notwithstanding the nature and seriousness of their crimes. Accordingly, the African Commission found a violation of article 3(2) of the African Charter due to Uganda's differential application of the Amnesty Act which, it claimed, occurred 'without any reasonable justification or explanation'. The African Commission also held that the state violated article 7(1)(a) and partially violated article 7(1)(d) of the African Charter due to the failure of the Supreme Court to provide reasons for staying the execution of the orders of the Constitutional Court and the unjustified delay in the hearing of the appeal before the Supreme Court. The African Commission found that the state had not violated articles 4, 5, 7(1)(b), (d), 16 and 26 of the African Charter as the complainant's claims therein were not reasonably established/supported.

Notably, the above communication is the first instance where the African Commission addressed the issue of amnesties in detail. The

African Commission in the section referenced as *obiter dictum* addressed the compatibility of the use of amnesty with the rights guaranteed in the African Charter. The Commission held that 'blanket or unconditional amnesties that prevent investigations ... are not consistent with the provisions of the African Charter', particularly where perpetrators are alleged to have violated those serious crimes referred to in article 4(h) of the AU Constitutive Act. The African Commission's jurisprudence in this respect serves as an important normative development in the area of transitional justice. Additionally, the African Commission's decision to address in *obiter* a matter otherwise unrelated to the contentions between the parties provides an exciting avenue for the development of African human rights jurisprudence, specifically those issues that are rarely litigated.

3.1.1 Positive developments

As regards positive developments, the African Commission highlighted the ratification of the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (African Women's Protocol) by South Sudan, Ethiopia and Tunisia as increasing the number of state parties to 42; the ratification of the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Older Persons (Older Persons Protocol) by the Kingdom of Lesotho; and the ratification of various United Nations (UN) instruments by state parties, including the Republic of The Gambia, which also deposited its declaration under article 34(6) of the Protocol to the African Charter on the Establishment of the African Court, enabling individuals and CSOs to directly refer matters to the Court.

Another aspect of the African Commission's work relates to the normative development of the law under the African Charter. The most important normative developments in the respective period were its adoption of the Draft Protocol to the African Charter on Human and Peoples' Rights on the Rights of Citizens to Social Security and Protection (Social Security Protocol); and the Study on Transitional Justice in Africa, which provides much-needed guidance to state parties on fulfilling their obligations under the African Charter during periods of transition. Additionally, the AU Assembly adopted the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Persons with Disabilities in Africa (African Disability Rights Protocol) in January 2018. The two Protocols serve as landmark instruments and were developed in collaboration with the AU Commission. Indeed, the adoption of the Disability Rights Protocol illuminates an oft-misunderstood field of human rights while the Protocol on Social Protection, once adopted by the AU Assembly, will effectively contribute to extending coverage for the vast majority of people in Africa that are otherwise not covered by any social protection provisions. Disturbingly, however, the use of 'citizens' in the title of the Social Protection Protocol seems to exclude other classes of persons. Bearing in mind the often-deplorable conditions of non-citizens in African states, the seemingly restrictive application could have deleterious effects. However, pending adoption by the AU Assembly and subsequent publication of the Protocol, the nature and effect of the prospective qualification cannot be appropriately discussed.

With regard to national judgments and the adoption of national laws, the African Commission highlighted the abolition of the death penalty in Burkina Faso and the proposed abolition in The Gambia; the decriminalisation of abortion in Rwanda; the adoption of a law against racial discrimination in Tunisia; the decriminalisation of defamation in the Kingdom of Lesotho and Rwanda, including the enactment by Seychelles of the Access to Information Act; the promulgation of a new Mining Code by the DRC in March 2018; and the decision of the High Court of Kenya in April 2018 which held that the installation of the Device Management System on mobile phone platforms would breach privacy and consumer rights. The Commission also highlighted the peaceful presidential elections in Egypt, Liberia and Sierra Leone, including the publication of an election date in the DRC.

3.1.2 *Areas of concern*

The areas of concerns highlighted in the African Commission's Activity Reports were the continued non-ratification of its instruments, the low levels of state reporting under the African Charter and the African Women's Protocol and the sparse implementation of its decisions and recommendations on communications/complaints, provisional measures and letters of urgent appeal. Substantive issues included the rise in conflict-related violations in Cameroon, Mali, Somalia, Libya and other parts of the Sahel; the extension of the death penalty in Mauritania and its continued use in Botswana, Egypt, Nigeria, Somalia and Sudan; attacks on press freedom in Kenya, Benin, Gabon and Mali, including the persistent shutting down of the internet and social media in Ethiopia, Chad, Cameroon and the DRC. Other issues included the humanitarian crisis in refugee camps in Cameroon following the flow of refugees from Nigeria and Central African Republic; post-electoral protests following the recent presidential elections in Mali; xenophobic attacks in South Africa; and frequent reprisals against human rights defenders in the DRC and Egypt. Structurally, due to inadequate staffing the African Commission continues to struggle to implement its mandates, an issue that has less to do with inadequate finances and more to do with the sluggish recruitment processes at the AU Commission. Consequently, the African Commission has failed to recruit a single staff member under the Pan-African Programme (PANAF) notwithstanding funding from the European Union (EU) for this purpose. The African Commission has repeatedly requested autonomy in recruiting staff, to no avail.

Another pressing concern relates to recent questions surrounding the African Commission's independence following its withdrawal of observer status from the non-governmental organisation (NGO) Coalition of African Lesbians (CAL). The African Commission's decision was adopted pursuant to Executive Council Decision EX.CL/Dec1015(XXXIII) of June 2018 on the recommendations of the Joint Retreat of the Commission and the Permanent Representative Council (PRC) which reiterated previous requests by the Executive Council for the withdrawal of CAL's observer status. Notably, where previous Executive Council decisions had requested the same, the African Commission had responded by avowing that CAL's observer status was 'properly' obtained and that the African Commission was committed to protecting the rights in the African Charter 'without any discrimination because of status or other circumstances'. Following a backlash against the African Commission by AU policy organs over the

Commission's perceived recalcitrance, the latter was requested to hold a Joint Retreat with the PRC in June 2018 resulting in the above-referenced decision. Accordingly, during its 24th extraordinary session, the Commission adopted a decision on the withdrawal of the observer status granted to CAL and notified the latter thereafter.

3.2 African Court on Human and Peoples' Rights

The African Court is the continental court established by the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights. Its mandate is to complement the mandate of the African Commission and to monitor the implementation of the African Charter and other human rights documents ratified by African countries. In 2018 the African Court delivered 18 judgments. For the purposes of this article, the case of the *Association Pour le Progrès et la Défense des Droits des Femmes Maliennes (APDF) and the Institute for Human Rights and Development in Africa (IHRDA) v Mali (APDF & IHRDA v Mali)* is discussed since it is the first time that any institution at the AU level has made a decision on the provisions of the African Women's Protocol.

The complainants in this case, APDF and IHRDA, alleged that, measured through the lens of human rights instruments, the 2011 Malian Family Code has many defects. First, it reduces the minimum age of marriage for females to 16, while retaining 18 for males, with even an exception for a girl to be married at 15 contrary to article 2 of the African Children's Charter and article 6(b) of the African Women's Protocol. Second, the Code neither obliges religious ministers to obtain both parties' consent prior to their marriage nor requires the presence of both parties at the ceremony, which transgresses article 6(a) of the African Women's Protocol and articles 16(a) and (b) of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). Third, it recognises the application of Mali's Islamic law in matters of inheritance, which gives women and girls half of what men receive, contrary to article 21(2) of the African Women's Protocol. Fourth, the Code sanctions Islamic law in Mali, which takes the position that children born out of wedlock are only entitled to inheritance if their parents so desire, contrary to articles 3 and 4(1) of the African Children's Charter. Finally, the applicants claimed that by introducing the Code, Mali had failed to comply with its positive obligation in eliminating traditions and customs that are harmful towards women and children as provided under article 1(3) of the African Children's Charter, article 2(2) of the African Women's Protocol and article 5(a) of CEDAW.

Responding to the allegations, the government of Mali stressed that its laws must mirror the 'social, cultural and religious realities' in the country and argued that it would be ridiculous to adopt laws that would be difficult to execute. It also strengthened its argument by stating that the Code was flexible in that the testator is free to manage their inheritance in other ways, for instance, according to the Code rules or their will, above and beyond religious or customary law, if they wish to do so. It further contended that the discontent and strife that had halted the promulgation of the prior 2009 Family Code, which enshrined an 'equal share for men and women with the participation of the children born out of wedlock in the devolution of estate on the same footing as the legitimate child' had

created a situation of fear 'where it felt it was not able to provide greater rights to women and children in family matters'.

After hearing both sides of the debate, the Court adopted and sanctioned the allegations of the applicants entirely and pronounced that the Code had transgressed all the alleged treaty provisions. In doing so, it rejected Mali's justification concerning the flexibility of the Code, saying that 'the Family Code in Mali enshrines religious and customary law as the applicable regime in the absence of any other legal regime'. The Court also vetoed Mali's argument that 'the established rules must not eclipse social, cultural and religious realities' within the country, recalling Mali's commitments to eliminate discrimination against women and children irrespective of existing cultural and religious practices and beliefs. The Court then ordered the government of Mali to amend the Code, harmonise its law with the international treaties, and inform and educate its people as to the rights and obligations enshrined therein.

This decision of the Court is noteworthy not only for being the first pronouncement by the Court on women's and children's rights, but also for upholding the obligation of states to adopt legislation, policies and practical measures to eliminate discrimination against women and children irrespective of existing cultural and religious practices and beliefs. The judgment will also have positive implications for women and children in other African states that adopt Islamic law either partially or fully as their legal regime. Further, given that the Court's decision is binding, its willingness to rule on the African Children's Charter, irrespective of its connection to a right stipulated under the African Charter, has the potential to strengthen the effective implementation of the African Children's Charter, thereby contributing to the realisation of children's rights on the continent.

That said, given that in Mali earlier efforts to comply with the provisions of the family law with human rights standards caused large-scale civil unrest; and following the Court's judgment, the Muslim associations of Mali regarded the Court's decision as an outrage to Mali's social and religious values and called on citizens to 'take action to save the country from this danger'. The Court should open dialogue with Mali and other states as well as non-state actors to implement the decision without disturbing public order.

3.3 African Committee of Experts on the Rights and Welfare of the Child

The African Children's Committee is the human rights organ of the AU that oversees the implementation of the rights and welfare of the child in Africa. This part focuses on developments within the African Children's Committee as it concerns communications, general comments and studies.

3.3.1 Communications

In terms of jurisprudence, the African Children's Committee becomes the first human rights monitoring body in the African human rights system to pronounce itself on the complicated issue of statelessness that arises in the process of state secession. The communication was submitted by two NGOs, the Centre of Justice and Peace Studies and People's Legal Aid

Centre (the complainants) on behalf of Ms Imam Hassan Benjamin against the government of the Sudan (*Iman v Sudan*).

Iman, who resides in Sudan, was born from a Sudanese mother, Hawa Ibrahim Abd al-Karim, and a South Sudanese father, Hasan Benjamin Daoud, in Alhasaheisa, a small town to the south of Khartoum. Upon completion of primary and secondary education, Ms Iman decided to apply for a university education. However, she could not do so as the university's enrolment rules required a person to have a national identity number, which she did not have. She then filed an application for a national identity card with Sudan's civil registration department. Her case was referred to the Aliens Persons department, stating that she no longer was a Sudanese citizen as her father's last name showed that he was from the Baria tribe, Yei district, what now is South Sudan, and that he would have become a South Sudanese national upon separation as per the 2011 amendments of the Sudan Nationality Act of 1994 which called for, among others, the automatic revocation of Sudanese nationality of those who *de facto or de jure* became citizens of the Republic of South Sudan with the effect that Sudanese nationality of a minor child would be rescinded when the nationality of one's 'responsible father' is revoked. The Act also proscribed dual nationality with South Sudan even though dual nationality with other countries is allowed.

The revocation of Ms Iman's Sudanese nationality occurred irrespective of the fact that her mother was Sudanese and her father, who had held Sudanese nationality and lived in Al-hasaheesa town of Sudan, where he married and served in the police force, passed away before the secession of South Sudan. So the only surviving parent at that time was her mother, who is a Sudanese.

On these bases, the complainants requested the African Children's Committee to declare that Sudan has transgressed the provisions of the African Children's Charter, specifically article 3 on the principle of non-discrimination, article 4 on the principle of the best interests of the child, and articles 6(3) and 6(4) on the right to acquire nationality and the obligation to prevent statelessness. The complainants also claimed, among others, consequential violation of the right to education.

In response, the Sudanese government contended that following the amendments made to the Act in 2005, a child was entitled to acquire Sudanese nationality from his or her Sudanese mother, on an equal footing with a Sudanese father. The respondent state further contended that section 10(2) of the Act, which provides for automatic revocation of Sudanese nationality of those who became citizens of South Sudan, does not have any discriminatory purposes, but rather is the result of political and legal arrangements, which South Sudan has also been applying.

After hearing both sides of the debate, the African Children's Committee found Sudan in violation of several obligations, notably protection against arbitrary deprivation of nationality, discrimination and against deprivation of access to education. On discrimination, the Children's Committee ruled that the Act was not aligned with the African Children's Charter as it states that every Sudanese can have dual nationality except the nationality of South Sudan, and this amounts to discrimination on the basis of country of origin. In this regard, the African Children's Committee rejected the respondent state's argument that South

Sudan is also doing the same to Sudanese nationals, stressing that state parties' obligations with regard to the African Children's Charter were not dependent on reciprocity. The African Children's Committee also found gender-based discrimination because while children of a South Sudanese mother and a Sudanese father have no difficulty acquiring Sudanese nationality, children born to South Sudanese fathers and Sudanese mothers are at risk of statelessness as they are required to go through an administrative process to be considered a Sudanese national by birth. Further, the African Children's Committee pronounced that the revocation of Iman's Sudanese nationality constituted arbitrary deprivation under articles 6(3) and 6(4) of the African Children's Charter because her father was not alive. Besides, Iman's father could not be considered a South Sudanese national *de jure* or *de facto* since at the time of his death there was no concept of South Sudanese nationality as he passed away before the secession of South Sudan. As regards education, the African Children's Committee ruled that the withdrawal of Ms Iman's Sudanese nationality denied her the opportunity to attend a higher education institution, and so violated article 11 of the African Children's Charter.

This decision of the African Children's Committee has paramount importance not only for being the first of its kind in the African human rights system to address the questions of nationality arising from the process of state secession, and providing relief to Iman, who was facing the risk of statelessness, but also for its positive implication for the rest of the children in a similar situation as the risk of statelessness in Sudan.

The African Children's Committee also made another ground-breaking judicial pronouncement in the year 2018 in the case of *Institute for Human Rights and Development in Africa and Finders Group Initiative (complainants) on behalf of TFA v the Government of Republic of Cameroon (TFA v Cameroon)*. This case concerned a 10 year-old child, identified as TFA, who was allegedly raped on 9, 12, 15 and 16 April 2012 in Bamenda, Cameroon, by Angwah Jephther, a wealthy and prominent man in the area. According to the complainants, even though TFA's family reported the crime to the local police, no measure was taken to detain the suspect, and the police took three months to file their investigation report. The examining magistrate rejected the case for lack of evidence despite the existence of convincing medical evidence that TFA had been raped and the fact that she also managed to identify the suspect's house as the crime scene. Furthermore, the examining magistrate refused to provide a copy of its written decision and hence the victim's counsel was unable to file an appeal. Moreover, TFA's counsel and her aunt were sued for defamation when they commented on the errors in the investigation. The complainants approached the African Children's Committee, asserting that the state's failure to adequately investigate the rape, or to allow an appeal against the magistrate's decision, violated several provisions of the African Children's Charter.

Even though the government of Cameroon contended that an appeal was underway to challenge the decision of the magistrate, the African Children's Committee denounced the argument stating that the appeal was unduly prolonged and was not in line with the best interests of the child. The African Children's Committee also rejected the respondent state's submission that psychosocial support had been given to the victim and her family, because in the view of the African Children's Committee the

government had failed to produce any reliable evidence to verify its claim. On these bases, the African Children's Committee declared that the respondent state's failure to bring the perpetrator to justice and provide the necessary support to the victim over the course of the five years indicated its failure to act with due diligence to investigate, prosecute and punish the perpetrator within a reasonable time and hence violated its obligation under article 1 of African Children's Charter. The African Children's Committee also found that the respondent state's lack of due diligence transgressed the non-discrimination principle of the African Children's Charter, stating that the crime of rape against the victim constituted gender-based violence, a form of gender-based discrimination in view of developments in international human rights law. It reached this conclusion considering the fact that the social subordination of women which causes and legitimises gender-based violence, which in turn affects women and nullifies the enjoyment of several of their human rights, by itself constituted gender-based discrimination. Finally, the African Children's Committee held that the respondent state contravened its obligation under article 16 of the African Children's Charter which, in its view, required state parties to undertake a thorough investigation and ensure that adequate compensation is given to the victims of child abuse and torture. The African Children's Committee therefore recommended that the government of Cameroon takes necessary measures to redress the violations of the African Children's Charter, including immediately bringing the offender to justice; paying the sum of 50 million CFA to TFA as compensation; and enacting and implementing legislation that eliminates all forms of violence against children.

The findings of the African Children's Committee in this case are noteworthy not only for being the first case of sexual violence on a minor decided at the regional level, but also for being a major plus to human rights jurisprudence in Africa. The African Children's Committee's interpretation of the due diligence standard in this communication is a deviation from the decision of the African Commission on sexual violence in the case of *Equality Now v Ethiopia*, where it held that a state's failure to investigate the sexual assault of a 13 year-old minor was a transgression of a state's due diligence obligations but did not amount to discrimination since the complainant failed to show a similarly situated person that benefited from better state protection.

3.3.2 General Comment

The African Children's Committee adopted its fifth General Comment on State Party Obligations under article 1 of the African Children's Charter in 2018. The General Comment is guided by the four core principles of the African Children's Charter, namely, non-discrimination; devotion to the best interests of the child; the right to life, survival and development; and the right to participation of children. Given that article 1 relates to all rights and protection contained in the African Children's Charter, the role of the General Comment to ensure the realisation of children's rights, thereby improving the living realities of children in Africa is beyond doubt. While it helps the African Children's Committee to expound its understanding of state party obligations under the African Children's Charter, it is important for making the same well understood by both governmental and non-governmental actors.

The General Comment sanctions that the rights set forth in the African Children's Charter are interdependent and inextricably intertwined, and socio-economic rights are justiciable in the same way as civil and political rights. It also makes clear that there is no reference in article 1 to the 'progressive realisation of rights,' or to the degree of realisation within the 'maximum extent'. Hence, states cannot invoke a lack of resources to justify non-implementation of the rights and standards in the African Children's Charter. The General Comment calls on state parties to comply at least with previously agreed targets relating to social spending such as the Abuja Declaration, which requires 15 per cent of gross domestic product (GDP) spending on health services and the Dakar Declaration which sets 9 per cent of GDP spending on education.

The General Comment further stresses that the meaning of the terms 'shall recognise' under article 1 is peremptory, underling the rights-based approach so that the implementation of the rights set forth in the African Children's Charter should not be seen as a charitable process. Of importance is that the General Comment also explains what 'legislative and other measures' entail pursuant to article 1 of the African Children's Charter.

3.3.3 *Studies*

Another important promotional activity of the African Children's Committee in 2018 is the launch of its comprehensive study entitled 'Mapping children on the move within Africa'. The study was undertaken following concerns around the continuous growing movement of children within Africa and respective challenges that they are facing while on the move. The finding of the study gives a synopsis of the situation of children on the move within Africa. It specifically provides an overview of the routes that children move in to and from the continent, pushing and pulling factors of the children on the move, challenges they are facing, normative and institutional mechanisms of African states to protect children on the move, and a way forward.

Regarding migration routes, the study mapped three main routes, which are routes within the Horn of Africa and out of the region, routes through the West and Central Africa into North Africa and the West African routes. Regarding the reasons why they move, the study recognised different pushing and pulling factors including conflict and insecurity, illegal activities such as smuggling, trafficking, economic and social factors such as poverty, forced marriage, climate change and a lack of education.

As far as challenges are concerned, the study found many issues such as discrimination, economic or sexual exploitation, neglect and violence, arbitrary arrest and deportation, loss of identity, name and nationality and denial of education and health service. Furthermore, on policy and institutional mechanisms, despite some sporadic efforts, there are weak legal and institutional mechanisms in various African states to safeguard children on the move. This relates to a lack of vibrant institutional standing on the concept of children on the move, the inadequacy of the legal regime to address challenges faced by children on the move, the absence of effective and efficient systems to trace children on the move, the lack of regional coordination and the existence of a one-size-fits-all method to deal with children on the move. Finally, as a solution the African Children's Committee called on member states, including state of

origin, transit and destination countries, to regard children on the move as children first irrespective of the reasons why they leave their homes, where they come from or where they are and how they got there; and to take all necessary measures, such as legislative and administrative measures, and provide all the support and facilities that children on the move need to thrive. If the recommendations of the study are effectively implemented, it has the potential to significantly improve the situation of children on the move in the African continent.

4 Conclusion

Overall, the developments in relation to democracy in Africa in 2018 reveal mixed outcomes, continuing the pre-2018 trend of what Cheeseman (2018) called the 'divided continent'. There has been evidence of a transition from authoritarianism towards a hopeful democratic beginning (Angola, Ethiopia, The Gambia); democratic progress (Sierra Leone, Burkina Faso); stagnation (Zimbabwe); and a relative decline (Tanzania and Zambia). While progress has been slow and opposition groups have faced pressure including in some of Africa's stable countries, such as Zambia, Senegal, Tanzania and Benin, and Africa's relatively low democratic standing, the continent has largely avoided the democratic recession narrative that has beset established democracies in other parts of the world. In fact, with the relative openings in some of the continents influential and formerly authoritarian states, such as Angola, Ethiopia, and recently the DRC, and potentially Algeria and Sudan, the trajectory may well be towards an African progress in democracy. Indeed, the 2019 Report of Varieties of Democracy Institute (V-Democracy), indicates that Africa is the only region that has avoided extensive 'autocriticism' in the form of substantial and significant worsening on the scale of liberal democracy. Nevertheless, the continent continues to be ranked among the worst in the world. Political leaders, regional and sub-regional organisations, civil society groups and, most importantly, the people of the continent should continue to push for the establishment and consolidation of democracy.

As for the judicial and human rights institutions at the AU level, there have been several positive developments such as cases/communications decided on issues of women's rights such as child marriage, inheritance rights and harmful practices, children's rights, statelessness, rape and discrimination. Moreover, soft laws in the form of General Comments and studies have been adopted by the institutions to guide states in the implementation of the provisions of the human rights instruments. These steps, including the progressive interpretation of the law in the case of statelessness and the obligations of the state, demonstrate that the judicial and human rights institutions at the AU level are progressing in terms of monitoring the implementation of human rights on the continent. However, these steps are minimal compared to the mountain of challenges that human rights in Africa face. Hence, these institutions must speed up their efforts to implement their mandates and keep adopting a progressive approach when interpreting the provisions of the law.

References

- Abebe AK 'Taming regressive constitutional amendments: The African Court as a continental (super) Constitutional Court' (2019) 17 *International Journal of Constitutional Law* 89
- Al Jazeera 'Sierra Leone opposition leader wins presidential election runoff' 5 April 2018, available at <https://www.aljazeera.com/news/2018/04/sierra-leone-opposition-leader-wins-presidential-election-runoff-180405050505118.html> (last visited 4 June 2018)
- Al Jazeera 'South Africa's Parliament elects Cyril Ramaphosa as President' 22 May 2019, available at <https://www.aljazeera.com/news/2019/05/south-africa-parliament-elects-cyril-ramaphosa-president-190522180418635.html> (last visited 4 June 2019)
- Bado K 'Togo's continuing constitutional crisis and ECOWAS's failed mediation effort' *ConstitutionNet* 30 January 2019, available at <http://constitutionnet.org/news/togos-continuing-constitutional-crisis-and-ecowass-failed-mediation-effort> (last visited 4 June 2019)
- Biryabarema E 'Uganda's top court upholds ruling on extending President's rule' *Reuters* 18 April 2019, available at <https://af.reuters.com/article/ugandaNews/idAFL5N2205ZA> (last visited 4 June 2019)
- Cheeseman N 'A divided continent: Regional Report Africa', BTI 2018, available at https://blog.bti-project.org/wp-content/uploads/sites/3/2019/02/BSt_BTI_2018_AfricaReport_Lay.pdf (last visited 4 June 2019)
- Dahir AL 'For the first time in decades, there are no Ethiopian journalists in prison' *Quartz Africa* 13 December 2018, available at <https://qz.com/africa/1494561/ethiopia-has-no-jailed-journalists-in-2018-the-first-since-2004/> (last visited 16 May 2019)
- Daily Mail 'Togo changes law to let President stand for two more terms' 9 May 2019, available at <https://www.dailymail.co.uk/wires/afp/article-7010165/Togo-changes-law-let-president-stand-two-terms.html> (last visited 4 June 2019)
- Fagbayibo B 'A case for democratic legitimacy of the AfCFTA process' *AfronomicsLaw* 17 January 2019, available at <http://www.afronomicslaw.org/2019/01/16/a-case-for-democratic-legitimacy-of-the-afcfta-process/> (last visited 4 June 2019)
- Feldstein S 'Zimbabwe's *coup* did not create democracy from dictatorship' *The Conversation* 16 August 2018, available at <https://theconversation.com/zimbabwes-coup-did-not-create-democracy-from-dictatorship-101510> (last visited 4 June 2019)
- Freedom House 'Freedom in the World 2019', available at https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf (last visited 4 June 2019)
- Heungoup H de M 'Cameroon's Anglophone crisis: How to get to talks?' *International Crisis Group Report 272/Africa*, 2 May 2019, available at <https://www.crisisgroup.org/africa/central-africa/cameroon/272-crise-anglophone-au-cameroun-comment-arriver-aux-pourparlers> (last visited 4 June 2019)
- Iheukwumere M 'Incorporating anticorruption measures in the African Continental Free Trade Agreement (AfCFTA)' *GAB: The Global Anticorruption Blog*, 24 May 2019, available at <https://globalanticorruptionblog.com/2019/05/24/incorporating-anticorruption-measures-in-the-african-continental-free-trade-agreement-afcfta/> (last visited 4 June 2019).

- Jeffery A 'Is Ramaphosa really a committed reformer?' *BizNews* 25 April 2019, available at <https://www.biznews.com/leadership/2019/04/25/ramaphosa-reformer-hype-jeffery> (last visited 4 June 2019)
- Kössler K 'Conflict and decentralisation in Mozambique: The challenges of implementation' *ConstitutionNet* 20 December 2018, available at <http://constitutionnet.org/news/conflict-and-decentralization-mozambique-challenges-implementation> (last visited 16 May 2019)
- Mekki N 'Local elections in Tunisia: Implementing the Constitution and reinforcing the transition' *ConstitutionNet* 1 June 2018, available at <http://constitutionnet.org/news/local-elections-tunisia-implementing-constitution-and-reinforcing-transition> (last visited 16 May 2019)
- News 24 'Burundi President surprises with vow to step down in 2020' 11 June 2018, available at <https://www.news24.com/Africa/News/burundi-president-surprises-with-vow-to-step-down-in-2020-20180609> (last visited 4 June 2019)
- Parmentier A 'Les enjeux du référendum constitutionnel aux Comores' *La Croix* 30 July 2018, available at <https://www.la-croix.com/Monde/Afrique/enjeux-referendum-constitutionnel-Comores-2018-07-30-1200958690> (last visited 4 June 2019)
- Posner D & Young D 'Term limits: Leadership, political competition and the transfer of power' in N Cheeseman (ed) *Institutions and democracy in Africa: How the rules of the game shape political developments* (2018) United Kingdom: Cambridge University Press 260
- Powell A 'Angolan President, one year in, praised for anti-corruption push' VOA 27 September 2018, available at <https://www.voanews.com/a/angola-president-anti-corruption-push/4589717.html> (last visited 4 June 2019)
- Ssemogerere K 'Uganda's age limit petition: Constitutional Court demurs on substance, cautious on procedure' *ConstitutionNet* 14 August 2018, available at <http://constitutionnet.org/news/ugandas-age-limit-petition-constitutional-court-demurs-substance-cautious-procedure> (last visited 4 June 2018)
- Trade Law Centre 'African Continental Free Trade Area (AfCFTA) Legal Texts and Policy Documents', available at <https://www.tralac.org/resources/our-resources/6730-continental-free-trade-area-cfta.html> (last visited June 2019)
- TRT World 'Ethiopia swears in Abiy Ahmed as PM amid hopes for peace' 2 April 2018, available at <https://www.trtworld.com/mea/ethiopia-swears-in-abiy-ahmed-as-pm-amid-hopes-for-peace-16410> (last visited 4 June 2019)
- Vandeginste S 'Burundi's constitutional referendum: Consolidating the *fait accompli* in the run-up to the 2020 elections' *ConstitutionNet* 23 January 2018, available at <http://constitutionnet.org/news/burundis-constitutional-referendum-consolidating-fait-accompl-run-2020-elections> (last visited 4 June 2019)
- V-Dem 'Democracy facing global challenges' Annual Democracy Report 2019, May 2019, available at https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf (last visited 4 June 2019)

Democracy and human rights developments in Southeast Europe during 2018

Odetta Berberi*

Abstract: *This article provides an overview of the developments in democracy and human rights during 2018 in the countries of Southeast Europe, focusing on nine countries. Different reports have revealed that the Southeastern European region is experiencing a regression as far as democracy and human rights are concerned. According to Freedom House, democracy is in retreat in many parts of the world, including in Europe. In this article the author highlights the main developments around democracy in three European Union (EU) member states: Romania, Bulgaria and Croatia. These countries continue to be listed as the worst performers in the EU in respect of adherence to the rule of law and widespread corruption. Six countries from the Western Balkans region – Albania, North Macedonia, Montenegro and Serbia are candidate countries, and Bosnia and Herzegovina and Kosovo – are analysed in respect of the latest developments relating to democracy and human rights. Since the regional dimension is very important for the Western Balkans, a part is dedicated to bilateral relations in the framework of EU integration.*

Key words: *European Union; Southeast Europe; democracy; human rights; enlargement*

1 Introduction

This article provides an overview of the developments in democracy and human rights during 2018 in the countries of Southeast Europe (SEE). Nine countries that have shown *similarities* concerning development pertaining to democracy and human rights are the focus of the article. Nevertheless, these countries are positioned *differently* in respect of their various paths towards European Union (EU) integration, and their status varies considerably, varying between being member states, candidate countries and potential candidate countries.

Romania, Bulgaria and Croatia are EU member states; Albania, North Macedonia, Montenegro and Serbia are candidate countries; and Bosnia and Herzegovina and Kosovo are potential candidate countries. Even among the candidate countries, there are 'frontrunners' such as Serbia and Montenegro which have been promised membership by 2025. As the prospect of EU membership is a key factor for reforms in the region, this article is organised as follows: The first part describes the main developments in democracy and human rights in EU member states, followed by the second part of the article that discusses the main developments in the Western Balkans (WB).

* PhD (Political Science) (University of Tirana, Albania); Researcher and Advisor of the Albanian Parliament on the EU integration issues; odetabe@gmail.com

In contrast to other regions of the world, in SEE¹ democratic and human rights development are influenced by the EU. The EU's monitoring mechanisms and 'stick-and-carrot' approach have been very influential factors in the region. Nevertheless, since the economic crises, followed by the migration crises, and the rise of nationalism within the EU, and the Brexit, the EU has placed the Balkans 'at the end of the agenda', in this way contributing to the rise of illiberalism among the countries of the region. This gap left by the EU has strengthened the influence of other actors such as Russia, China or Turkey (Heath 2018). European Commissioner Johannes Hahn stated in an interview in July 2018 that he was most concerned about China, as the Chinese are attempting to export their way of life, entailing 'a combination of capitalism with dictatorship' (Politico 2018).

2 EU member states: Rumania, Bulgaria and Croatia

Southeast Europe is composed of countries that are members of the EU and countries that aspire to become members of the organisation. In this part the author analyses the development of democracy and human rights in three countries of SEE that are members of the EU. Democratic backsliding in the last years has become the main topic for the EU and scholars who have started researching on the reversibility of the Europeanisation achievements in the member states. Hungary was the first to be criticised for its constant attack on democratic institutions, followed by Poland. In September 2018 the European Commission had to refer Poland to the European Court of Justice (ECJ) for the adoption of a new law on the Supreme Court, which was considered in conflict with the principle of judicial independence (Marović, Prelec & Kmezić 2019: 46).

Even though Romania and Bulgaria have been members since 2007, because of concerns over certain issues, the EU monitoring mechanisms continue to work under the 'Cooperation and Verification Mechanism' (CVM) (Marović, Prelec & Kmezić 2019: 45).

Starting with Romania, the year 2018 registered developments that have further undermined democracy and the progress made by the country, especially in the field of strengthening the rule of law. The outcome of the 2016 parliamentary elections brought to power the Social Democratic Party. In February 2017 protests erupted in Romania against the government's proposed changes in judicial systems and the decriminalisation of corrupt offences. This protest was considered the largest protest since the fall of Communism. Following this massive protest, other protests were repeatedly held during 2017. The events at the beginning of 2017 created a general mistrust in the ruling party (Freedom House 2018). In December 2017 the Romanian Parliament adopted three laws reforming the judiciary system. Critics claimed that this put under attack the system of checks and balances in Romania. The most supported opinion by the

1 The geographical region of South-East Europe has experienced modifications regarding dependence of the states that are considered part of it. Following the enlargement of 2007, the EU refers to the region of South-East Europe as composed of the successor states to the former Yugoslavia (with the exclusion of Slovenia) plus Albania. Following the enlargement of Croatia in 2013, the region of South-East Europe as defined by the EU is composed of six countries of the Western Balkans.

Romanian Constitutional Court, which it adopted in October 2017, is that most of the changes proposed by the government are unconstitutional (European Parliament 2018). The Romanian Minister of Justice in February 2018 initiated the dismissal procedure for the head of the National Anticorruption Directorate (DNA), Laura Codruta Kovesi (The Romanian Journal 2018). The Superior Council of Magistracy and the President did not support this decision (The Romanian Journal 2018). The constitutional conflict between the Justice Minister and the President was 'solved' by the Constitutional Court of Romania, which decided that the President should sign the decree to recall Kovesi from office (The Romanian Journal 2018). In April the Council of Europe's Group of States against Corruption (GRECO) expressed serious concern about the laws adopted by the Romanian Parliament.

Furthermore, the Venice Commission in its opinion in October 2018 came to the conclusion that the draft could undermine the independence of the judiciary. The same conclusions by the Venice Commission and GRECO were emphasised by the Commissioner for Human Rights of the Council of Europe during her visit to Romania in November 2018. She expressed her concerns that the weakening of the judiciary could result in the weaker protection of human rights to the authorities (Commissioner for Human Rights 2018: 24). In 2018 general protests continued to oppose government changes to the judicial system. Meanwhile, the ruling party ousted the second Prime Minister in seven months and designated Viorica Dăncilă as Prime Minister. The protest of 10 August 2018, which was supported by Romanians working abroad, ended in hundreds of protesters being injured (The Guardian 2018). According to the human rights reports of the US State Department, more than 770 protesters filed complaints concerning violent incidents during the protest of 10 August (US Department of State 2018).

In the meantime the Social Democrat-led government survived a confidence vote in December 2018 for not reaching the required quorum 50 per cent plus one of the votes (EUROACTIV 2018). Freedom House in its report 'Freedom in the world 2019' continued to rate the country as 'free' (Freedom House 2019). However, in line with the same report in one year, the scores in civil liberties and political rights declined (Freedom House 2019: 16).

In this context of political contestation, the situation of human rights in Romania appeared problematic. Of the 82 rulings against Romania adopted by the European Court of Human Rights in 2018, 37 were for 'inhuman or degrading treatment' and 18 rulings concerned the judiciary branch (the right to a fair trial and the duration of proceedings) (ECHR 2018: 177). In the report of 2018 the Commissioner for Human Rights of the Council of Europe focused on the rights of persons with disabilities, violence against women and the reform of the judicial system. In the first two issues under consideration, the Commissioner urges the authorities to take measures in order to fight discrimination and stigma that both categories face, and for the judiciary reform the Commissioner highlighted the concerns expressed by GRECO, the Venice Commission and other internal actors (Commissioner for Human Rights 2018).

In the meantime, in the European institutions, concerns about the above-mentioned developments were voiced and discussed in different sessions of the European Parliament (EP). According to Frans

Timmermans, first Vice-President of the Commission, in his speech before Parliament in October 2018 stated:

We are following the latest developments in Romania with concern ... We have seen substantial progress in the past, but things are now moving backward in a way that would be damaging for the place that Romania has built as an EU member state in recent years.

The European Parliament in its Motion for a Resolution on the Rule of Law in Romania of November 2018 expressed concerns about the rule of law in Romania, affected by the redrafted legislation on the judiciary and the political restrictions on media freedom. Finally, the language of the European Commission on the progress in Romania under the Cooperation and Verification Mechanism for the period covering November 2017 to November 2018 was very demanding (European Commission 2018). The Commission stated (European Commission 2018: 17):

The entry into force of the amended justice laws, the pressure on judicial independence in general and on the National Anti-Corruption Directorate in particular, and other steps undermining the fight against corruption have reversed or called into question the irreversibility of progress.

To remedy the situation, the Commission recommended to the Romanian authorities not to implement the justice laws that entered into force during 2018. However, the rule of law criterion was regarded by the EP as not linked to the Schengen Agreement. For this reason the European Parliament in November 2019 adopted a report in favour of the entrance of Romania and Bulgaria into the Schengen area and urged the Council to confirm the entrance of both countries into the area (European Parliament 2018).

Bulgaria is the second country to become a member state in the 2007 enlargement. Freedom House in its report 'Freedom in the world 2019' continued to rate the country as free (Freedom House 2019). According to the same report, in one year the scores in civil liberties and political rights did not undergo any change (Freedom House 2019: 16). The European Commission in its latest report concerning the progress of the country in CVM mentioned that 2017 was characterised by 'unfavourable conditions', listing government instability, media freedom and unpredictability in the legislative process as the main factors for undermining the reform process in Bulgaria (European Commission 2018: 1). Instead, the year under review (November 2017 to November 2018) was considered favourable as it 'helped' progress in reforms and especially in the adoption of a framework on the anti-corruption reform. The Commission mentioned media freedom as an issue of concern as it can affect the judicial reform and in a larger dimension the good governance (European Commission 2018: 2). The Commission concluded that the year 2018 was very positive in terms of implementing the recommendations of the previous report. For this reason, three benchmarks were provisionally closed (European Commission 2018: 11). Even though the Commission explained that democracy or media freedom was not the object of the CVM reporting, scholars raised concerns over the optimistic rhetoric of the EU institutions when referring to Bulgaria. The killing of a Bulgarian journalist, Victoria Marinova, also raised concerns, as her last report was about the misuse of EU funds. The Commissioner of Human Rights of CoE and Human Rights

Watch also raised concerns about the need to address violence against women and girls in Bulgaria (Commissioner for Human Rights 2018).

At the same time, concerning human rights developments, according to the European Court of Human Rights (ECHR), in 2018, in 29 rulings against Bulgaria, eight rulings concern the judicial branch (the right to a fair trial and the duration of proceedings) (ECHR 2018: 177). Human rights organisations reported widespread discrimination of Roma communities. A phenomenon mentioned by human rights organisations operating in the country was the segregation of entire schools enrolled by Romani children (US Department of State 2018).

Finally, this part concludes with Croatia, which managed to become the twenty-eighth member state of the EU and was considered a success story for the rest of the Western Balkan (WB) region. As the country had to cope beforehand, in the pre-accession period, with the concerns of the judicial sector, the Cooperation and Verification Mechanism was not availed in the case of Croatia. Freedom House in its report 'Freedom in the world 2019' continued to rate the country as free (Freedom House 2019). Nevertheless, according to the same report, in one year the scores in civil liberties and political rights declined (Freedom House 2019: 16). The World Justice Project (WJP) in its 2019 rule of law-index, lists five countries as the worst performers in the EU from the perspective of ordinary citizens (World Justice Project 2019: 21). Apart from the latest countries that joined the EU (Bulgaria, Croatia, Romania), Greece and Hungary joined the 'club' of the worst performers. In the 2019 report of the European Commission on Croatia's progress on structural reforms, it was stated that '[s]ome steps have been taken to improve the judiciary ... Backlogs in the courts are decreasing, especially in respect of the oldest cases, but remain sizable' (European Commission 2019: 14). In the same Report, the European Commission stated that the fight against corruption remained an issue of concern, with no improving trend even for 2018 (European Commission 2019: 57).

3 Western Balkans: Two steps ahead and three steps backward

Freedom House in its report 'Freedom in the World 2019', which refers to the period under consideration in this article, namely, from 1 January 2018 to 31 December 2018, points out that there is a decline in democracy and human rights in Europe (Freedom House 2019). Democracy is endangered by anti-democratic leaders in Central Europe and the Balkans who continue 'undermining institutions that protect freedoms of expression and association and the rule of law' (Freedom House 2019).

Scholars argue that the EU and the enlargement process shape developments relating to democracy and human rights in the Western Balkans region. For the Western Balkans the last year has been full of significant events in many directions. I will explore the developments in the Western Balkans countries in three main dimensions: internal developments, bilateral relations, and EU-WB relations. I start with the relations between the Western Balkans region, as the changes in these relations have had their relevance in the internal developments in democracy of each country.

3.1 European Union and Western Balkans relations in 2018

As far as the relations between the EU and WB are concerned, in the last year important developments were registered. The current situation of the WB as regards EU membership is as follows: Two of the six WB countries have opened accession negotiations, namely, Montenegro since 2012 and Serbia since 2014. The Republic of North Macedonia² has been a candidate country since 2005 and Albania obtained candidate status in 2014. The last two countries, Bosnia and Herzegovina (BiH) and Kosovo, are potential candidates. Being two contested states, the enlargement process has encountered a further obstacle. In order to progress in this process, according to Hahn, BiH should overcome the 'Dayton logic', which remains in place in the country.

The most important developments of the relations EU-WB in 2018 started with the release in February by the European Commission of a document titled 'A credible enlargement perspective for an enhanced EU engagement with the Western Balkans', in which the EU rounded off what a clear enlargement for the WB region meant. What is to be noted from the document is the wide range of criteria formulated in this round of enlargement. European Commissioner Johannes Hahn stated in an interview in July 2018 that lessons learned from previous accessions (Rumania and Bulgaria) brought to demand sustainable democracy for the countries that wished to become EU members (Politico 2018).

Four areas were identified: the rule of law; economic development; bilateral disputes; and enlargement is a matter of choice, meaning as long as there is a clear and wide internal support of the EU perspective. In the above-mentioned document, the region was divided into the so-called 'front-runners', Serbia and Montenegro, which potentially could be EU members by 2025, leaving the other countries without a prospect date of accession.

In April 2018 the EU Commission released the Enlargement Package and the individual progress of WB countries. Recognising the efforts of Albania, especially as far as justice reform was concerned, and that of Macedonia in resolving bilateral disputes, the Commission recommended to the EU Council the opening of negotiations with both countries. Meanwhile, BiH could become a candidate country and Kosovo could benefit of visa liberalisation and advance on the path towards EU membership, only after the normalisation of the situation with Serbia.

The first half of 2018 was followed by two important events: the EU-Western Balkans Summit in Sofia, which took place in May 2018; and the London Summit of the Berlin Process which was held in July 2018. The Sofia Summit was concluded with the signing of the Sofia Declaration that reaffirmed, 15 years after the Thessaloniki Summit of 2003, the EU perspective of the Western Balkans. Meanwhile, one month before the London Summit two events took place: the Prespa Agreement, and the Council decision to postpone the opening of the negotiations with Albania and North Macedonia in 2019. These events were reflected in the London Summit and in the documents that were signed. Importance was given to

2 Following the agreement with Greece and the referendum of September, the official name of Macedonia is the 'Republic of North Macedonia'. In this article I will continue to use the shorter version of Macedonia.

the peaceful resolution of bilateral disputes in the region and the previous achievements in this direction were welcomed and defined as positive progress.

The second half of 2018 was also marked by important developments in EU-WB relations. Following years of efforts by Kosovo on visa liberalisation, the European Commission confirmed the completion of all the requirements under this process in July 2018, and in September the European Parliament voted in favour of visa liberalisation with Kosovo. Nevertheless, the finalisation of this process halted in the European Council, as it has not as yet taken any decision on this matter.

What is to be noted from the events of 2018, in the framework of EU-WB relations, is the importance given to the resolution of the bilateral disputes through peaceful means. As a matter of fact, 2018 registered important developments concerning bilateral relations in the Western Balkans region. After three decades of disagreements between Greece and the former Yugoslav Republic of Macedonia, regarding the so-called 'name issue', the two countries reached an historic agreement in June 2018. Furthermore, developments were registered between Greece and Albania.

As far as the negotiations between Macedonia and Greece were concerned, following an intense year of negotiations the two countries on 17 June 2018 reached an historic agreement. This agreement was supported by important actors of the international community, the EU and the US, as it has put an end to nearly three decades of the so-called 'name dispute'. After the agreement of June some complex and important steps followed. First it required the ratification in parliament of both countries which, considering the resistance by factors inside the countries, was not an easy process. Nevertheless, on 5 July 2018 the Macedonian Parliament ratified the agreement and a referendum was called for Macedonian citizens for 30 September. The referendum had a low turnout and those who participated voted in favour of the name change. Following the referendum, Parliament voted in favour of initiating the constitutional revisions, which required a two-thirds majority. The government started the process of drafting four constitutional amendments that were discussed in the Macedonian Parliament in December. These amendments must be adopted in Parliament by a two-thirds majority.

Meanwhile, Albania and Greece intensified the negotiations in 2018. The bilateral relations between the two countries are considered complex. Even though both countries are members of the North Atlantic Treaty Organization (NATO), Greece still formally has in force a 'state of war' with Albania. According to the former Albanian Minister for Europe and Foreign Affairs during his reporting on 28 February 2018 in the Commission of Foreign Affairs of the Albanian Parliament, Albania is negotiating with Greece a 'package' made up of different issues. The ending of the 'state of war' with Albania, which has importance for the Cham community, the delineation of the maritime border, the rights of the Greek national minority that lives in Albania, and textbook revision, are some of the topics mentioned as 'open issues' and are on the table of negotiations between the two countries. Nevertheless, in February 2018 the President of the Republic of Albania refused a government request to authorise continued negotiations with Greece on the delineation of the maritime border with the justification to have full information on the content of the negotiations (BIRN 2018). In March the President granted

authorisation for continuing negotiations with Greece. Following this decision, the two foreign ministers met several times during 2018 but it is expected that the negotiations will continue in 2019.

3.2 Internal developments of the countries of Western Balkans

In this part of the article each country is analysed in depth concerning developments around democracy and human rights. The European Parliament is the EU institution that constantly addresses shortcomings in democracy openly and directly. In November 2018 the European Parliament adopted resolutions on every country of the WB region, except for BiH, due to the country disagreements on establishing a Joint Stabilisation and Association Parliamentary Committee. What can be noted from the text of the resolution is the fact that the region still faces serious problems concerning the rule of law, corruption, state capture, organised crime and the lack of economic development.

Montenegro has been considered one of the countries that has advanced more on the European path. Nevertheless, in the EP Resolution of November 2018 on the Montenegro Progress Report, important challenges that need to be addressed immediately are 'the rule of law, media freedom, corruption, money laundering, organised crime and its associated violence' (EP Resolution 2018: 3). Following the parliamentary elections of 2016, the Democratic Party of Socialists (DPS) won 36 seats and form the majority with the other four parties. The outcome of the election was not accepted by the opposition, which initiated a parliamentary boycott that partially ended in December 2017. As the presidential elections were approaching, in February 2018 Johannes Hahn, Commissioner for European Neighbourhood Policy and Enlargement Negotiations, visited Montenegro and addressed the members of parliament of the country. The commissioner reaffirmed decisively that the accession of Montenegro was unquestionable and highlighted the role of Parliament and that of civil society to press the government to continue on the EU path (EWB 2018). After postponements and internal discussions, in March the Assembly of Kosovo ratified the Border Demarcation Agreement with Montenegro. It was considered good news by international actors, and the EU considered it one of the major achievements which could lead to visa liberalisation.

In April 2018 the presidential elections took place in Montenegro. These elections were organised in an atmosphere of parliamentary boycott by the opposition for not recognising the results of the 2016 general elections (ODIHR 2018: 3-4) Mr Đukanović won the election in the first round with a vote of 53,9 per cent. According to the final report of the OSCE/ODIHR Election Observation Mission, the elections were assessed as democratic and fundamental freedoms were respected. However, shortcomings were identified and some recommendations that needed to be addressed as a matter of priority were formulated (for instance, the review of the legal framework for the next elections, addressing all allegations of electoral violations, further reinforcing the transparency of the electoral process, taking measures to protect journalists, and so forth) (OSCE/ODIHR 2018: 21). In the Resolution adopted in November 2018 the European Parliament called on Montenegro to foster a climate of tolerance, to take measures against hate speech and to ensure the inclusiveness of minorities (EP Resolution 2018: 7).

In the case of Serbia, in the Resolution of November 2018 on the Commission Report the EP emphasised freedom of expression and the independence of the media as a serious concern (EP 2018: 3). According to the document the rule of law, the fight against corruption and the fight against organised crime remained issues of concern even during 2018. As far as the quality of democracy in Serbia was concerned, the EP emphasised the need for the Serbian Parliament to effectively conduct an 'oversight of the executive, and that the transparency, inclusiveness, and quality of the legislative process need to be further improved' (EP 2018: 6). In order to further uphold human rights in Serbia, the EP recommended that it is needed a climate of tolerance and all types of hate speech needed to be condemned. Respect for and the protection of minorities were highlighted issues on which Serbia needed to further work for an effective implementation of the strategy that has been adopted in this matter. Meanwhile, in the section of regional cooperation, the European Parliament urged Serbia and Kosovo to continue their engagement in dialogue. The EP expressed concerns about the debates on exchanges of territories as it must not affect the multi-ethnic nature of both states (EP 2018: 10). Good neighbourhood relationships are important for Serbia on its European path, meaning that the opening issues with Croatia had to be overcome. In February 2018 the two Presidents of Serbia and Croatia met in Zagreb, where salient issues such as the Danube River and war compensations that should be paid by Serbia were discussed. Both Presidents declared after the meeting that there was a common will to solve the open issues, despite their different attitudes on these matters (EWB 2018).

As far as Albania was concerned, the EP in its Resolution expressed deep concern over the *de facto* boycott of the opposition since summer 2018, which undermined the constructive political dialogue required for 'the implementation and consolidation of the reforms across all five key priorities are vital to the effort to advance the EU accession process and for the proper functioning of a democratic regime'. According to the European Commission the rule of law remained a key challenge for Albania. The justice reform initiated in 2017 continued to register good progress (European Commission 2018). The International Monitoring Operation (IMO), which conducts the vetting process of judges and prosecutors across the country, had delivered approximately 100 decisions during 2018 (Calavera 2018). In October 2018 two new organs of the judiciary were established: the High Judicial Council and the High Prosecutorial Councils.

The US Department of State in 2019 published its annual report on human rights practices in 2018 in Albania. The report identified as a big concern the 'pervasive corruption in all branches of government' and the phenomena of impunity, minority rights and the problem of property rights. During 2018 Albania updated its legislation on anti-corruption and was advancing in the establishment of the National Bureau of Investigation, the Special Tribunal and the Special Prosecution Office Against Corruption and Organised Crime (European Parliament 2018). As far as the protection of minorities is concerned, Albania was continuously improving its legislation on minority rights protection. Following the approval of the specific law on national minorities in November 2017, the country is continuing the process of approving bylaws on the implementation of the Framework Law on National Minorities. Three

bylaws have so far been approved, namely, the Council of Ministers Decision 561 dated 29 September 2018 relating to primary education; the Council of Ministers Decision 562, dated 29 September 2018 on the promotion of minority languages and culture in tertiary education; and the Decision of Council of Ministers 726 dated 12 December 2018 on the organisation of the Committee on National Minority. Instead of addressing concerns on property rights, in 2018 the Law 111/2018 'On Cadaster' was approved by Parliament. In the Law 'On Cadaster' the establishment in 2019 of the State Agency of Cadaster was foreseen which would merge with different agencies that already existed and would try to address concerns over propriety rights.

In the Republic of North Macedonia, after noticing the decisive commitment of the country on the EU path, the European Parliament remained concerned about media freedom, corruption and organised crime, even though the EP pointed out in the document that corruption and organised crime were widespread in the region and were an issue of concern even in the last two countries, namely, Kosovo and BiH. The European Parliament noticed that the country had advanced more in good neighbourly relations and had achieved a high level of *acquis* alignment (EP 2018). The second half of 2018 was dominated by the implementation of the Prespa Agreement with Greece and the preparation for NATO membership of the country. In December 2018 the leader of the Albanian party DUI, Ali Ahmeti, launched the idea of a consensual candidate for President (Radio Evropa e Lirë 2018). Ahmeti's proposition was supported by the Prime Minister, Zoran Zaev, who initiated talks with coalition parties over a consensual candidate for President. This practice was considered a very important development for democracy in Macedonia, taking into account the recent approach of President Ivanov vis-à-vis ethnic Albanians in the country.

The last two countries, Kosovo and Bosnia and Herzegovina, because they are considered contested states,³ this element poses a very important challenge to the Europeanisation process. Specifically in Kosovo, the EP in its Resolution adopted in November was concerned about elements of state capture, the rule of law and inter-ethnic relations. Nevertheless, what has kept the EU and international attention were the developments that had repercussions on the negotiations with Serbia. The first half of 2018 was marked by tensions, following the murder of the Kosovo Serbian politician Oliver Ivanović and the proposals of 'border corrections' between Kosovo and Serbia which could lead to a final agreement. The second half of 2018 exacerbated the relations between the two countries as both countries took initiatives that damaged the achievements of the negotiation process. The efforts by Serbian diplomacy to revoke the recognition of Kosovo's independence was followed by the government of Kosovo's decision to impose in November 2018 a 100 per cent tariff on goods emanating from Serbia and Bosnia and Herzegovina. The latest decision taken by the government in Kosovo was criticised by the EU that demanded its revocation.

3 Contested state for the purposes of this article is defined as a state that is contested internally by a segment of the population and this contestation is supported externally by an external actor (Serbia) which supports this contestation in both cases.

In Bosnia and Herzegovina the EP Resolution was adopted in February 2019. The EP emphasised the fact that ethno-nationalistic rhetoric had dominated the political discourse and had halted 'the constitutional, political and electoral reforms that would transform BiH into a fully effective, inclusive and functional state based on the rule of law'. The year 2018 was a year of elections in Bosnia and Herzegovina. According to the OSCE/ODIHR Election Observation Mission the general elections in BiH of 7 October 2018 took place 'in an atmosphere of political disillusionment with public institutions and characterised by a lack of economic growth' (OSCE/ODIHR 2018: 4-5). In his final report ODIHR listed irregularities prior to and after election day. Furthermore, *Radio Free Europe* reported multiple cases of deceased persons remaining on the voter registry, which could lead to possible electoral manipulations (Radio Free Europe 2018).

Milorad Dodik, the former President of the entity Republika Srpska for two full terms, won the elections and become a Serb member of the country's three-member presidency. His party also had a victory in the Republika Srpska's presidency and took the majority of seats in Republika Srpska's Assembly. In the Federation of Bosnia and Herzegovina, the Party for Democratic Action (SDA), representing the Bosniak ethnic group and the Croat Democratic Union of Bosnia and Herzegovina (HDZ BiH) representing Croats, won the majority. As a priority recommendation the OSCE/ODIHR mission identified the need to address the European Court's judgments regarding discriminatory ethnicity (OSCE/ODIHR 2018: 25).

4 Conclusion

The year 2018 registered important developments that questioned the reversibility of the achievements of the Europeanisation process in the cases of Romania and Bulgaria. The European Commission continued to have in place a mechanism for monitoring the situation in the two countries, because for more than a decade these countries failed to fight widespread corruption and continuing threats to the rule of law. The Western Balkans countries continued to register a decline in democracy towards an overly 'formal' version of democracy and Europeanisation, characterised by adopting norms and rules without fully implementing and enforcing these norms. In the latest report of European Commission, state capture, corruption and organised crime were considered key concerns that contributed to the decline in democracy. At the regional level, positive developments can be noted, which may contribute to the stability of the region. The historic agreement between Macedonia and Greece has opened a new era for the bilateral relations in the conflict-ridden region of the Western Balkans. It is to be expected that, during 2019, other bilateral disputes would similarly find a peaceful resolution.

References

- BIRN 'Albania President blocks talks on sea border with Greece' (February 2018), available at <https://balkaninsight.com/2018/02/20/albania-president-blocks-negotiations-over-sea-border-with-greece-02-20-2018/> (last visited 5 March 2019)
- Commissioner for Human Rights of the Council of Europe 'Commissioner's statement on the murder of Bulgarian journalist Victoria Marinova' (October 2018), available at <https://www.coe.int/en/web/commissioner/-/commissioner-s-statement-on-the-murder-of-bulgarian-journalist-victoria-marinova> (last visited 5 March 2019)
- Commissioner for Human Rights of the Council of Europe 'Report following her visit to Romania from 12 to 16 November 2018' (2018), available at <https://rm.coe.int/report-on-the-visit-to-romania-from-12-to-16-november-2018-by-dunja-mi/1680925d71> (last visited 10 February 2019)
- European Commission 'Report from the Commission to the European Parliament and the Council; on Progress in Romania under the Cooperation and Verification Mechanism' COM/2018/851 (2018), available at <https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52018DC0851> (last visited 22 February 2019)
- European Commission 'A credible enlargement perspective for and enhanced EU engagement with the Western Balkans' (February 2018), available at https://ec.europa.eu/commission/sites/beta-political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf (last visited 20 March 2019)
- European Commission 'Enlargement package: Commission publishes reports on the Western Balkans partners and Turkey' (April 2018) press release, available at http://europa.eu/rapid/press-release_IP-18-3342_en.htm (last visited 20 March 2019)
- European Commission '2018 Communication on EU Enlargement Policy' (April 2018), available at https://ec.europa.eu/commission/sites/beta-political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf (last visited 20 March 2019)
- European Commission 'Key findings of the 2018 Report on Albania' (April 2018), available at http://europa.eu/rapid/press-release_MEMO-18-3403_en.htm (last visited 20 March 2019)
- European Commission 'Country Report Croatia 2019 including an in-depth review on the prevention and correction of macroeconomic imbalances' (2019), available at https://ec.europa.eu/info/sites/info/files/file_import/2019-european-semester-country-report-croatia_en.pdf (last visited 15 March 2019)
- European Court of Human Rights 'Annual Report' (2019), available at https://www.echr.coe.int/Documents/Annual_report_2018_ENG.pdf (last visited 25 March 2019)
- European Parliament 'Resolution of 29 November 2018 on the 2018 Commission Report on Serbia' (2018), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0095+0+DOC+XML+V0//EN&language=EN> (last visited 20 March 2019)
- European Parliament Plenary debate on the Rule of Law in Romania (October 2018), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20181003+ITEM-003+DOC+XML+V0//EN&language=EN> (last visited 12 February 2019)

- European Parliament 'Motion for a Resolution, the Rule of Law in Romania' (November 2018), available at http://www.europarl.europa.eu/doceo/document/B-8-2018-0522_EN.pdf (last visited 12 February 2019)
- European Parliament 'Resolution of 29 November 2018 on the 2018 Commission Report on Albania', available at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2018-0481> (last visited 20 March 2019)
- European Parliament 'Report on the full application of the provisions of the Schengen acquis in Bulgaria and Romania: abolition of checks at internal land, sea and air borders' (November 2018), available at http://www.europarl.europa.eu/doceo/document/A-8-2018-0365_EN.html?redirect (last visited 12 February 2019)
- European Parliament 'European Parliament resolution of 13 November 2018 on the rule of law in Romania' (2018), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0446+0+DOC+PDF+V0/EN> (last visited 25 March 2019)
- EU Western Balkans Summit 'Sofia Declaration' (May 2018), available at https://www.consilium.europa.eu/media/34776/sofia-declaration_en.pdf (last visited 5 March 2019)
- European Western Balkans 'Speech by Commissioner Johannes Hahn at the Parliament of Montenegro' (February 2018), available at <https://europeanwesternbalkans.com/2018/02/09/speech-commissioner-johannes-hahn-parliament-montenegro/> (last visited 25 March 2019)
- European Western Balkans 'Serbia and Croatia to use opportunity to improve relations' (February 2018), available at <https://europeanwesternbalkans.com/2018/02/23/serbia-croatia-use-opportunity-improve-relations/> (last visited 20 March 2019)
- Freedom House 'Freedom in the World 2019: Democracy in Retreat' (2019), available at https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf (last visited 25 March 2019)
- Freedom House 'Nations in transit' (2018), available at <https://freedomhouse.org/report/nations-transit/2018/romania> (last visited 20 March 2019)
- EURACTIV 'Romanian government survives no confidence vote' (December 2018), available at <https://www.euractiv.com/section/politics/news/romanian-government-survives-no-confidence-vote-2/> (last visited 10 February 2019)
- Hillary Margolis 'Speak out to protect Bulgaria's women, European bodies should act to counter misleading' Dangerous Judgment, Human Rights Watch (October 2018), available at <https://www.hrw.org/news/2018/10/10/speak-out-protect-bulgarias-women> (last visited 5 March 2019)
- ODIHR 'Bosnia and Herzegovina general elections 7 October 2018, Final Report', available at <https://www.osce.org/odihr/elections/bih/409905?download=true> (last visited 20 March 2019)
- OSCE/ODIHR Montenegro presidential election 15 April 2018, Final Report (2018), available at <https://www.osce.org/odihr/elections/montenegro/386127?download=true> (last visited 5 March 2019)
- Radio Free Europe 'U BiH i mrtvi na spisku za glasanje' (October 2018), available at <https://www.slobodnaevropa.org/a/bosna-i-hercegovina-izbori-glasanje-29538508.html> (last visited 20 March 2019)
- Radosveta Vassileva 'Is Bulgaria the EU's next rule of law crisis?' EU Observer (September 2018), available at <https://euobserver.com/opinion/142795> <http://neweasterneurope.eu/2018/09/27/bulgarias-autocratic-model/> (last visited 25 March 2019)

- Ryan Heath, Andrew Gray 'Beware Chinese Trojan horses in the Balkans, EU warns', Politico (2018), available at <https://www.politico.eu/article/johannes-hahn-beware-chinese-trojan-horses-in-the-balkans-eu-warns-enlargement-politico-podcast/> (last visited 25 March 2019)
- The Guardian* 'Hundreds injured in Romania protests as emigrants return to fight corruption' (August 2018), available at <https://www.theguardian.com/world/2018/aug/11/hundreds-injured-in-romania-protests-as-emigrants-return-to-fight-corruption> (last visited 10 February 2019)
- The Romanian Journal 'Update 2: Justice Minister announces start of procedures to dismiss DNA chief Kovesi' (2018), available at <https://www.romaniajournal.ro/politics/update-2-justice-minister-announces-start-procedures-dismiss-dna-chief-kovesi/> (last visited 25 March 2019)
- The Romanian Journal 'CSM issues negative opinion on Justice Minister's call to dismiss DNA's Kovesi', (2018), available at <https://www.romaniajournal.ro/society-people/update-csm-issues-negative-opinion-on-justice-ministers-call-to-dismiss-dnas-kovesi/> (last visited 25 March 2019)
- The Romanian Journal 'President Iohannis says NO to Min's request to dismiss DNA head Kovesi. Minister Toader says will challenge decision to CCR, judicial disputes surface' (2018), available at <https://www.romaniajournal.ro/politics/update-president-iohannis-says-no-to-jusmins-request-to-dismiss-dna-head-kovesi-minister-toader-says-will-challenge-decision-to-ccr-judicial-disputes-surface/> (last visited 25 March 2019)
- The Romanian Journal 'CCR releases reasoning of ruling urging Kovesi's dismissal' (June 2018), available at <https://www.romaniajournal.ro/politics/ccr-releases-reasoning-of-ruling-urging-kovesis-dismissal/> (last visited 25 March 2019)
- US Department of State 'Country reports on human rights practices for 2018 in Bulgaria' (2018), available at <https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper> (last visited 5 March 2019)
- US Department of State 'Country reports on human rights practices for 2018: Romania' (2018), available at <https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper> (last visited 10 February 2019)
- World Justice Project 'Rule of Law Index 2019' (2019), available at https://worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2019_Single%20Page%20View-Reduced_0.pdf (last visited 5 March 2019)
- Western Balkans Summit 'Joint Declaration on Regional Cooperation and Neighbourly Relations in the Framework of the Berlin Process', available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724294/180710_WBS_Joint_Declarations.pdf (last visited 23 March 2019)