UNIVERSITA' COMMERCIALE "LUIGI BOCCONI"

PhD SCHOOL

PhD program in Legal Studies

(curriculum: International Law and Economics)

Cycle: 32nd

Disciplinary Field (code): IUS/08

The Interplay between National Security and Freedom of Expression Online in the Post-Soviet Countries

Advisor: Oreste POLLICINO

PhD Thesis by

Oleg SOLDATOV

ID number: 3026985

Academic Year 2019/2020

Acknowledgements

I would like to express my heartfelt gratitude to all those who have supported and encouraged me on the way to completing this project. First of all, profound thanks to my thesis supervisor, Professor Oreste Pollicino, who provided direction and focus at every stage of my work, along with invaluable advice and wise solutions to seemingly insoluble problems. I am also grateful to Professors Laurent Manderieux and Yane Svetiev for their availability to discuss my concerns about the scope and delimitations of this work, and to the administrative team of Bocconi University for their constant assistance during the course of this doctoral research.

I also benefited enormously from discussions with fellow researchers and human rights activists in the Faculty of Social Sciences of the Sao Paulo University; at YUCOM – the Lawyer's Committee for Human Rights (Belgrade); in the Faculty of International Relations of the Belarusian State University; and in the Shepard Broad College of Law of the Nova Southeastern University. Additionally, I would like to thank Ms Anna Sliesarieva, a Master's student in Digital Media and Society, Uppsala University, for her valuable contributions and suggestions.

I owe debts of gratitude to my former tutors at the University of Ghent Law School and the Stockholm School of Economics, who taught me perseverance and persistence in remaining analytical, and in striving to perceive the forest behind the trees.

Last but not least, I am thankful to my family for their staunch support throughout my academic journey.

Contents

1. Introduction

The time taken to research this thesis (2015-2019) coincided with the ongoing tectonic changes in the traditional global landscape of political, economic, social, and technological settlements. The era of certainties, of clear and indisputable definitions and meanings, and logical cause and effect interdependencies within the confines of critical thinking seem to have given way to a new vocabulary, such as retreat of reason,[1] crisis of democracy, hybrid wars, sovereign Internet, political fusion, use of big data, hard and soft power, innovative authoritarianism,[2] and online surveillance, to mention only a few. The technological progress and, specifically, the Internet that operates across all spheres of human existence, tend to erase boundaries between the real and the virtual, thereby complicating the already complex and obscure world panorama. The ubiquity of prompt online communication has transformed not only lives of individuals but also the ways communities are organised, how the banking sector operates, how education functions, how the government communicates, how military operations are mounted, or how justice is administered. Not surprisingly, these sweeping technological developments have had a significant impact on the way that citizens can realise or experience their fundamental rights, including the right to freedom of expression. By their very existence, the easily available virtual online instruments and tools can challenge an individual's value-based integrity in the face of a tsunami of information. And in a similar fashion, online communication tools test the resilience of public institutions, including those dealing with security and safety in this most unsafe world, and examine their capability to remain law-abiding and committed to serving their citizens. This interaction between the citizens and the state mediated by the Internet provides for a

[1] See, generally, Anthony Browne, *The Retreat of Reason: Political Correctness and the Corruption of Public Debate in Modern Britain* (The Institute for the Study of Civil Society 2006).

[2] Jarmo Kikstra, 'Authoritarian Regimes and Innovation: A Case Study' [2016] University College Twente <https://www.researchgate.net/publication/318404915_Authoritarian_regimes_and_innovation_a_case_study> accessed 5 October 2019.

fascinating arena in which to observe or to study the most recent trends in society: namely, the interplay between state security policies and the fundamental human right to freedom of expression.

For his study, the researcher selected a group of post-Soviet countries: Armenia, Azerbaijan, Belarus, Estonia, Georgia, Kazakhstan, Kyrgyzstan, Russian Federation, Ukraine, Uzbekistan. Although operating within a broader environement of the Communist Estern bloc, with a trendsetter located in the Kremlin, the researcher, for the clarity and cohesion focus on a range of the post-Soviet contexts. The selected countries have a common background related to their historical alignments with the Soviet Union. The truth, however, is that the length, depth, and scope of ideological influence, suppression, and subordination varied considerably across the group, as did the stages of their evolution into civilised societies: compare, for example, Estonia and Uzbekistan. After the collapse of the Soviet Union, the countries morphed into quite different sovereign states, economically, politically, socially, and technologically, with different centres of global attractions and alliances.

The author's working hypothesis is that regardless of individual historical paths − and despite differences in political and institutional regimes − there exists a commonality of Internet regulation practices that is shared by most of the countries. The researcher eschewed the bias to interpret the commonality and seeming interconnectedness as being due exclusively to prior relationships with the authoritarian regime, and remained open to the results as they unfolded throughout the analysis. The author tested his proposition by examining the shared context in the listed countries, and by systematically scrutinising the instances of legislative similarities, and, at times, the patterns of cross-fertilisation of legislative practices in the region.

To set the stage, this work presents the research design and methodology before moving on to describe the context in the post-Soviet region as well as linkages between the

countries in question. Possible reasons for the interconnectedness are described, such as regional authoritarian trends, frozen conflicts, and geopolitical narratives prevalent in the area. Sub-regional groups of states are presented to better prepare the reader for the discussion of practices curtailing freedom of expression across the region.

Next, the work takes a detour from the post-Soviet region to introduce the definitions of national security, terrorism, extremism, and freedom of expression as well as the interplay of these issues. It also explores the way emerging Internet technologies have changed the playing field when it comes to the expression of views that are both legally acceptable and potentially a threat to national security.

The author then briefly presents the existing good practices, drawing mostly upon the experiences of the 'old' democracies, before moving on to explore case studies conducted in the post-Soviet space. The scope of legislative interventions in the countries of the region is examined through the lens of the legitimisation of questionable practices of curtailing online expression and, subsequently, the methods employed, such as the takedown of information, deanonymisation, mass surveillance, and compartmentalisation of the Web.

This thesis presents an example of a multidisciplinary approach, drawing mainly upon legal studies, but it also cites research in the fields of political science and sociology, and factors in as necessary the technology-related subjects. A short technical glossary is provided at the end of the document.

2. Research Design and Methodology

2.1. Research Hypothesis

The previous body of research in this area had a tendency to address the role of information and communication technology, using the dual paradigm of liberation and repression, and often missing the subtleties of the middle ground. Diamond[3] notes that within the liberation purview information technologies allow citizens to report news and express opinions, cover offences, hold authorities to account, mobilise protest activities, and enhance participation. However, the benefits of the information and communication technology rendered to the citizens constitute just one side of a coin. The other side entails vast opportunities and options that technological advances can provide to autocratic regimes. Authorities have in their possession a wide assortment of methods and tools: for example, to overregulate the Internet,[4] to develop sophisticated filtering and controlling mechanisms,[5] and to identify dissenters by means of surveillance equipment,[6] to name just a few.

The author's hypothesis is that − regardless of the present-day political and institutional regimes − there exists a common range of predominantly repressive Internet regulation practices that is shared by the majority of the post-Soviet countries, and that have been introduced with specific reference to national security concerns.

For the purposes of this study, the selection of states is limited to the following countries: Armenia, Azerbaijan, Belarus, Estonia, Georgia, Kazakhstan, Kyrgyzstan, Russian Federation, Ukraine, and Uzbekistan. Temporally, the work covers the period from 2004 until the present time (mid-2019).

---

[3] Larry Diamond, 'Liberation Technology' (2010) 21 Journal of Democracy 69, 70.
[4] Espen Geelmuyden Rød and Nils B Weidmann, 'Empowering Activists or Autocrats? The Internet in Authoritarian Regimes' (2015) 52 Journal of Peace Research 338.
[5] Diamond (n 3) 70.
[6] Rød and Weidmann (n 4) 340–341.

In this research, the concepts of 'common practice' and 'legislative cross-fertilisation' will be disaggregated, with a particular focus on the use of the following legislative tactics that seem to be gaining popularity among legislators:

- a unique approach to legitimising limitations to freedom of expression with reference to national security-related issues (anti-extremism, anti-terrorism, criminal defamation laws when it comes to extending specific protection to state agents, and specifically worded anti-fake news legislation);
- unique procedures and measures related to the pre-emptive deanonymisation of all or certain categories of Internet users, requiring them to disclose their real identities to the authorities even in the absence of any indication of illegal activities;
- unique procedures and measures related to mass surveillance and data localisation.

Verification of the hypothesis regarding the commonality of Internet regulation tactics will be conducted through an analysis of all relevant legislative frameworks. The information will also be analysed vis-à-vis political developments in the post-Soviet states that are increasingly demonstrating features of authoritarian regimes.[7] In a range of instances, the research argues, anti-national security concerns might be smoke screens used by politicians to gain legitimacy, with the aim of further reducing freedom of expression in order to fortify their subservient political systems.[8]

2.2. Methodology

The research methodology is based on a multi-disciplinary and multi-dimensional approach. In particular, it departs from the pure 'black letter law' research tradition, and

[7] Grzegorz Ekiert, Jan Kubik and Milada Anna Vachudova, 'Democracy in the Post-Communist World: An Unending Quest?' (2007) 21 East European Politics and Societies 7.
[8] Nate Anderson, *The Internet Police: How Crime Went Online, and the Cops Followed* (WW Norton & Company 2013).

draws upon a wider selection of views on the topic expressed by the following informants: specialists in areas of human rights, rule of law, and media and information technology. The sources will cover various sectors such as private and governmental as well as academia and civil society.

Conceptually, the research relies in equal parts on learning through abstract conceptualisation by exploring the possible strategies of post-Soviet legislators (normative approach) and by learning through reflective observation (empirical approach). The empirical part of the research was pursued by way of gathering available information and data and lead by the interviews the author had with a number of stakeholders in the sector.

The desk review included the following sources:

- case law and legislative sources (both national and transnational);
- primary non-legislative sources (observation, engagement with online IT-related forums worldwide);
- secondary non-legislative sources (planning documents, meeting minutes, user agreements, and disclaimers published by online intermediaries) from pre-selected legal entities and external agencies;
- academic literature.

In addition to working within the framework of the Bocconi University PhD Programme in legal studies, the author carried out a significant part of the desk review in Sao Paulo (Faculty of Social Sciences of the Sao Paulo University); in Belgrade, Serbia (under the auspices of 'YUCOM – Lawyer's Committee for Human Rights'); in Minsk, Republic of Belarus (Faculty of International Relations of the Belarusian State University); and in Fort Lauderdale, the United States (Shepard Broad College of Law, Nova Southeastern University).

The interviews were unstructured, and their direction was led largely by the emergent questions on the agenda of cyberlaw of the countries under scrutiny. The selection of interviewees was drawn from the author's extensive network, built at the time of his employment at the Council of Europe. The interviews were conducted with government officials, legislators, and representatives of NGOs and Internet intermediaries both in Central/Western Europe (in person) and in other Council of Europe member states (via Skype/teleconferencing and, where viable, study trips). Based on the empirical data gathered, the synthesised case studies were compiled and an interpretation of the totality of information was undertaken. These studies played a central role in this project.

It is hoped that the research results and their interpretation will provide a sufficiently persuasive set of conclusions in line with the purpose of the research. In pursuit of this research journey, the working assumption has been that a level of anti-extremism protection similar to what has currently been attained in Eastern Europe could be achieved by measures that are less restrictive of the rights to privacy and free speech.

3. Context: The Post-Soviet Region from 1990 until 2018

This chapter explains the geographical delimitations of the present research project, and provides a contextual background that will subsequently be used in an analysis of the regional frameworks in Internet regulation.

3.1. Chasing Ghosts of the Past

The 20th century was an eventful albeit a tormenting and challenging period, packed with two world wars, dehumanising experiences of fascism and Stalinism, heinous examples of genocide, the establishment of new international entities (European Union, NATO, the UN, and the Council of Europe, to name a few), associations and dissociations of state entities, the advent of the Internet and a whole new virtual world, globalisation, perceived 'clashes of civilizations'[9] and a short-lived concept of the 'end of history'.[10] In many ways, the agenda of the 21st century was shaped by what had happened in the previous century, and some present-day phenomena (including the focus of this work) call for a retrospective look to give plausible responses to the developments of today. The past is haunting the present with its demons of pride and ghosts of glorious past history. Both for historians and politicians, a short historical distance can interfere with objective interpretations of past events and unbiased solutions to present-day predicaments, as the paradigms and conventions of the past have not been abandoned. The guiding principles, clichés, and discursive certainties that served well in previous years are still welcome attachments today. One such historical 20th-century event was the demise of the communist ideology in the 1980s, with the

[9] Huntington referred to cultural and ideological identities as dominant reasons for conflict in the post-Cold War world. According to him, the tensions remained between nations, even though the ideological war had ended. See P Samuel, *Huntington, The Clash of Civilizations and the Remaking of World Order* (Simon and Schuster 1996).

[10] 'End of history' is a philosophical concept that suggests history will become unchanging at some point due to some ultimate goal having been achieved. In the post-Cold War world, the concept was associated with the final victory of Western liberal civilisation. Francis Fukuyama articulated the latter approach in an article in 1989, and then in a book; see Francis Fukuyama, *The End of History and the Last Man* (Free Press 1992).

resultant 'stagnation' and unavoidable collapse of the Soviet Union in 1991. With the stabilising glue of the all-encompassing ideology removed − having served for over 70 years − the political, economic, social, institutional, cultural, and ethnical settlements started to crumble. With a total of 15 republics and 20 autonomous entities, and a population of 286.7 million,[11] the USSR was at some stage a global player, and one of the two nodes of world power *vis-à-vis* the US.

The transformation of a multi-national poly-confessional, and highly centralised entity started as a painful centrifugal process of fragmentation into its constituent parts, which was labelled 'a parade of sovereignties'. [12] For the former republics, it was a fearful and formidable political shift towards nation and state building,[13] while for individuals populating the USSR, it meant grappling with overwhelming new concepts of individual freedoms, doing away with cosy paternalistic attachments, stretching personal boundaries, and coming to terms with new constraints.

The dissolution of the Soviet Union was accompanied by a falling economy and the necessity of painful reforms.[14] States had to build new foreign policy tools and strategies to apply them to address consequences . Moreover, newly established states faced many challenges concerning national identities, historical narratives, and relationships with other

[11] Number retrieved from James Hughes and Gwendolyn Sasse, *Ethnicity and Territory in the Former Soviet Union: Regions in Conflict* (Routledge 2014).

[12] Henry E Hale, 'The Parade of Sovereignties: Testing Theories of Secession in the Soviet Setting' (2000) 30 British Journal of Political Science 31; Jeff Kahn, 'The Parade of Sovereignties: Establishing the Vocabulary of the New Russian Federalism' (2000) 16 Post-Soviet Affairs 58; Jeffrey Kahn, 'What Is the New Russian Federalism?' [2001] Contemporary Russian Politics: A Reader 374.

[13] Ronald Suny, *The Revenge of the Past: Nationalism, Revolution, and the Collapse of the Soviet Union* (Stanford University Press 1993).

[14] Arkady Moshes and András Rácz, 'What Has Remained of the USSR: Exploring the Erosion of the Post-Soviet Space' (Finnish Institute of International Affairs 2019) 58 65 <https://www.fiia.fi/wp-content/uploads/2019/02/fiia_report58_what_has_remained_of_the_ussr_web.pdf> accessed 12 September 2019.

parts of the world – which had to be reevaluated upon independence. [15] The need to reconsider the connections between former Soviet republics was an even bigger challenge.[16]

A range of differences can be noted across regional groups. The states can be divided into geographical and geopolitical criteria.[17] Further in this chapter the author scrutinises New Eastern Europe, Baltic, South Caucasus, Central Asia regions, and Russia as a major power. These groups – and individual states – represent a variety of foreign policy choices and objectives.

New Eastern Europe – represented by Ukraine, Belarus and Moldova – is the region that faces the hardest tension between EU and Russian geopolitical agendas.[18] Following the USSR disintegration, South Caucasus region - which comprises Georgia, Armenia and Azerbaijan - faced both internal and external challenges.[19] While internal challenges were associated with ethnic conflicts, statehood creation and economic transition, external challenges steamed from geopolitical competition over the region and entering new powers, such as the US, EU, Turkey, Iran and Russia.[20] But what did it mean for the Russian Federation, which ceased to play the role of uniting core and leading actor within the communist empire?

British professor Timothy Garton Ash expressed the view, for instance, that Russia should reinvent itself and find a new role. This process, thinks the historian, will take a long time.[21] In reality, after the disintegration of the USSR, the Russian Federation initially

---

[15] ibid.
[16] ibid.
[17] ibid 66.
[18] Daniel Hamilton and Gerhard Mangott, *The New Eastern Europe: Ukraine, Belarus, Moldova* (Center for Transatlantic Relations Washington, DC 2007) 1–3.
[19] Fareed Shafee, 'New Geopolitics of the South Caucasus' (2010) 4 Caucasian Review of International Affairs 184.
[20] ibid.
[21] Mykola Siruk, 'Ukrayina maye otrymaty chitku perspektyvu chlenstva v ES [Ukraine should get a clear prospect of EU membership - Timothy Garton Ash]' (*The Day*, 11 June 2019)

adopted the 'end of history' theory, trying to drift along in the neoliberal direction, using the vocabulary of 'transition'. However, by the 2000s, this period of fluidity of choice came to a close. The collapse of the USSR was referred to by President Vladimir Putin as a catastrophe,[22] thereby re-instating the discourse of capturing past glory, re-appropriating the language of 'rising from one's knees', and choosing a unique Russian route and promoting the 'Russian World' in contrast to the European values of equality, freedom, human rights, and solidarity.

A vast body of knowledge has been contributed by philosophers, historians, political study specialists, social scientists, and development practitioners to unravel these processes and to shed light on the complex change as well as the numerous sticking points and enigmas of post-Soviet transformations.[23] That particular theme, however, is not the subject of this research.

For the purpose of this study, the agenda can be simplified into two spheres of political turbulence the Russian Federation has had to face:

- Reinstating its leadership role in the post-Soviet territories. This ambition is in tandem with the country's global objective to speak on a par with heavyweights such as the EU, US, and China. This is linked ostensibly to the need to preserve a diplomatic language of 'zones of influence' and a successful blockage of the former republics in their progress towards the influence of Western institutions.

- Coping with uncertainties and risks relating to the globalised world and fighting terrorism. Eliminating threats to the security of the Russian Federation. It

---

<https://day.kyiv.ua/uk/article/svitovi-dyskusiyi/ukrayina-maye-otrymaty-chitku-perspektyvu-chlenstva-v-yes> accessed 25 June 2019.

[22] 'Putin Calls Collapse of Soviet Union "Catastrophe"' (*The Washington Times*, 26 April 2005) <https://www.washingtontimes.com/news/2005/apr/26/20050426-120658-5687r/> accessed 25 June 2019.

[23] Jordan Gans-Morse, 'Searching for Transitologists: Contemporary Theories of Post-Communist Transitions and the Myth of a Dominant Paradigm' (2004) 20 Post-Soviet Affairs 320; Fukuyama (n 10); Samuel (n 9).

should be borne in mind that this is a very real concern of every country in the world. The year 2001 proved a great milestone for President Putin when, after the events of 9/11, the Russian Federation emerged as the greatest ally of the US in its combat against anti-terrorism.

After the dissolution of the USSR, its territory became the arena for multiple influences and security-related challenges of a political, ethnical, religious, migration, and social mobility nature. With the expansive encroaching of the Internet and social networks, all governments began to give special weight to the rules of the game.

It should be noted that the two spheres of turbulence do not exist in separate compartments with clear-cut boundaries between them. It is important to understand that the language of anti-terrorism can be employed when challenges are in fact connected to responses to domestic public and political developments. By the same token, solutions of an anti-terrorism nature can be a smoke screen using the vocabulary commonly held to voice domestic public policy concerns.

3.2. Regional Authoritarianism

It should be noted that the European influence did not fully erase the long authoritarian tradition across the former Soviet Republics.[24] The historical roots can be traced back even to before the USSR, to the time of the Russian Empire, which included the majority of the states under scrutiny. As of 2019, the region remains a poor adherent to international standards of civil rights and political liberties.[25] Russia, Belarus, Kazakhstan,

[24] David R Cameron and Mitchell A Orenstein, 'Post-Soviet Authoritarianism: The Influence of Russia in Its "Near Abroad"' (2012) 28 Post-Soviet Affairs 1.
[25] 'Eurasia' (*Freedom House*) <https://freedomhouse.org/regions/eurasia> accessed 25 June 2019.

Uzbekistan, and Azerbaijan were indicated in freedom rankings as being 'not free'.[26] Most of the regimes established after the Soviet Union's collapse remain unchanged up to the present. Vladimir Putin has held the office of President of Russia since 2000 – with only a short-term break between 2008 and 2012, when he held the post of Prime Minister.[27] He is currently serving a fourth presidential term.[28] Alexander Lukashenko has served as President of Belarus since 1994,[29] and is already in his fifth presidential term. Because of its established regime, Belarus is commonly referred to as 'Europe's last dictatorship'.[30] Nursultan Nazarbayev was a Kazakh president from 1991-2019[31] when he took the unexpected decision to resign.[32] Nevertheless, he has been granted extensive power to influence politics under the 'Law on the Leader of the Nation'.[33] Islam Karimov served as President of Uzbekistan for 27 years − from 1990 until his death in 2016.[34] The first Kyrgyz President, Askar Akayev, held

[26] Only four countries in the region − Georgia, Moldova, Armenia, Ukraine − are not included in the 'not free' list. See 'Freedom in the World 2018' (*Freedom House*, 13 January 2018) <https://freedomhouse.org/report/freedom-world/freedom-world-2018> accessed 25 June 2019.
[27] Michel Eltchaninoff, *Inside the Mind of Vladimir Putin* (Oxford University Press 2018).
[28] 'Muted Western Reaction to Putin Poll Win' (19 March 2018) <https://www.bbc.com/news/world-europe-43455950> accessed 25 June 2019.
[29] 'Belarus — The World Factbook' (*Central Intelligence Agency*) <https://www.cia.gov/library/publications/the-world-factbook/geos/bo.html#Govt> accessed 25 June 2019.
[30] Sigrid Rausing, 'Belarus: Inside Europe's Last Dictatorship' *The Guardian* (7 October 2012) <https://www.theguardian.com/world/2012/oct/07/belarus-inside-europes-last-dictatorship> accessed 25 June 2019; Peter Pomerantsev, 'Why Europe's Last Dictatorship Keeps Surprising Everyone' *Washington Post* (25 March 2017) <https://www.washingtonpost.com/news/democracy-post/wp/2017/03/25/why-europes-last-dictatorship-keeps-surprising-everyone/> accessed 25 June 2019; 'Belarus's Lukashenko: "Better a Dictator than Gay"' *Reuters* (4 March 2012) <https://www.reuters.com/article/us-belarus-dicator-idUSTRE8230T320120304> accessed 25 June 2019.
[31] 'Background on Nursultan Nazarbayev' (*Carnegie Endowment for International Peace*, 26 March 2012) <https://carnegieendowment.org/2012/03/26/background-on-nursultan-nazarbayev-pub-47648> accessed 25 June 2019; 'Kazakhstan' (*Human Rights Watch*) <https://www.hrw.org/europe/central-asia/kazakhstan> accessed 25 June 2019.
[32] Olzhas Auyezov, 'Kazakhstan's Leader Nazarbayev Resigns after Three Decades in Power' *Reuters* (20 March 2019) <https://www.reuters.com/article/us-kazakhstan-president-idUSKCN1R01N1> accessed 25 June 2019.
[33] INFORM.KZ, 'Law on the Leader of the Nation' published in the official press of the republic' (*INFORM.KZ*, 15 June 2010) <https://www.inform.kz/ru/article/2278166> accessed 19 June 2019.
[34] 'Uzbek Strongman's Death Confirmed' (2 September 2016) <https://www.bbc.com/news/world-asia-37260375> accessed 25 June 2019.

the post for the period 1990-2005 until he was ousted as a result of the Tulip Revolution.[35] Ilham Aliyev has held the Azerbaijani Presidential office since 2003, after inheriting the position from his father.[36]

The right to be elected to a presidential post for an unlimited number of terms is enshrined in the constitutions of these republics.

In Belarus, constitutional amendments lifting restrictions on the number of presidential terms were adopted in 2004. The Central Election Commission announced that 79% of voters gave a positive answer to the referendum question:

> *Do you allow A. Lukashenko, the first President of the Republic of Belarus, to participate in the election for President of the Republic of Belarus, and accept the following amendments to the first part of Article 81 of the Constitution of the Republic of Belarus: 'The president is elected for five years directly by the people of the Republic of Belarus on the basis of universal, free, equal and direct suffrage by secret ballot?'* [37]

In reality, these are two separate questions. The Council of Europe Venice Commission concluded that the amendments are in direct contradiction to European democratic standards.[38]

---

[35] Dennis Kavanagh and Christopher Riches (eds), 'Askar Akayev', *A Dictionary of Political Biography* (Oxford University Press 2009) <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095358830> accessed 25 June 2019.

[36] Kagyz Toguzbayev, 'Prezidenty s vozmozhnostyami pozhiznennogo pravleniya [Presidents with life-long rule opportunities]' (*Radio Free Europe/Radio Liberty Azerbaijani Service*, 12 April 2018) <https://rus.azattyq.org/a/pozhiznennye-praviteli-postsovetskoye-prostranstvo/29160961.html> accessed 26 June 2019.

[37] 'Announcement of the Central Commission of the Republic of Belarus on Elections and the Conduct of Republican Referenda on the Results of the Republican Referendum on October 17, 2004 (Archieved)' (23 October 2006) <https://web.archive.org/web/20061023120330/http://rec.gov.by/refer/refer2004result.html#> accessed 26 June 2019.

[38] Venice Comission, Opinion on the Referendum of 17 October 2004 in Belarus 2004 [CDL-AD(2004)029].

According to Article 81 of the Constitution of the Russian Federation, 'One and the same person may not be elected President of the Russian Federation for more than two terms running'.[39] The vagueness of this provision, however, makes it possible for a president to run multiple times.[40] Since 2008, the Presidential term in office has increased from 4 to 6 years.[41]

Article 42 of the Constitution of the Republic of Kazakhstan rules that the same person cannot be elected president for more than two terms; however, this restriction does not apply to the First President.[42]

The Constitution of Uzbekistan restricts election of the same candidate to more than two terms.[43] Nevertheless, In 2015, when Islam Karimov ran for the post a third time, officials gave the following explanation:

> *the notion of "term" means the exact number of years and, as the previous presidential term was seven years while the next will be five years, these cannot be considered as two consecutive terms*.[44]

In 2009, the provision on the limitation to two presidential terms was excluded from the Azerbaijani Constitution. Currently, Ilham Aliyev is serving his fourth term as president.[45]

---

[39] The Constitution of the Russian Federation ch 4.
[40] 'Podryad na podryadyu: Kakoye slovo nuzhno ubrat' iz Konstitutsii [Two in a row: What word should be removed from the Constitution]' (*Novayagazeta.ru*, 17 February 2018) <https://www.novayagazeta.ru/articles/2018/02/17/75540-podryad-na-podryad> accessed 26 June 2019.
[41] Federal Law 'On changing the term of office of the President of the Russian Federation and the State Duma' 2008 [6-FKZ].
[42] Constitution of the Republic of Kazakhstan 2019.
[43] Catherine Putz, 'Karimov, Uzbekistan's Perpetual President' (*The Diplomat*, 11 April 2015) <https://thediplomat.com/2015/04/karimov-uzbekistans-perpetual-president/> accessed 26 June 2019.
[44] 'Limited Elections Observation Mission: Republic of Uzbekistan – Presidential Elections, 29 March 2015' (OSCE 2015) <https://www.osce.org/odihr/elections/uzbekistan/148186?download=true> accessed 26 June 2019.
[45] Toguzbayev (n 36).

3.2.1. From the Cold War to the 'Cold Peace' (1990s)

Despite the fact that Russia's position was considerably challenged by other international players in the aftermath of the USSR's dissolution, the Russian Federation undoubtedly remains the leading and the strongest actor in the region, striving to reclaim the past glories of the Soviet Empire.

As was highlighted in previous sections, during the first post-Soviet years, Russia continued to pave its way in accordance with Gorbachev's slogan of 'new political thinking' and democratisation doctrine. The short-lived ideological mainstream of neoliberal ideology at the time offered President Boris Yeltsin and Foreign Minister Andrei Kozyrev no alternative other than to drift towards Western financial assistance and the integration of Russia into Western institutions.[46] However, the crisis in Yugoslavia became a critical point at which to re-evaluate the 'Atlanticist' vector in the Kremlin's foreign policy, and to articulate its own geopolitical priorities. Already in 1992, Yeltsin's initial support of Western initiatives in the Bosnian war was met with domestic pressure and opposition. Yeltsin and Kozyrev were criticised for serving the West instead of pursuing Russia's national interests.[47] Under these conditions, the official rhetoric shifted to having more sympathetic undertones with regard to Serbia − Russia's historical ally.

Following the launch of NATO's Partnership for Peace programme in 1994, which was intended to expand the alliance in the Central and East European region, the Russian Federation felt even more disappointed by its Western partners. At the meeting in Budapest in 1994, Yeltsin warned that 'just after Europe got rid of the Cold War legacy, it risks plunging into the Cold Peace'.[48]

---

[46] Andrei P Tsygankov, *Routledge Handbook of Russian Foreign Policy* (Routledge 2018) 69.
[47] Predrag Simic, 'Russia and the Conflicts in the Former Yugoslavia' (2001) 1 Southeast European and Black Sea Studies 95; Tsygankov (n 46) 248.
[48] Strobe Talbott, *The Russia Hand: A Memoir of Presidential Diplomacy* (Random House 2007) 141.

The ultimate reversal from a brief Atlantic bias in Russian foreign policy was associated with the appointment of a new Foreign Minister, Eugeny Primakov, in 1996. He took a more pragmatic approach towards Western countries, and instead put considerable effort into strengthening relations within the Commonwealth of Independent States (CIS). The shift was easily justified *vis-à-vis* strengthening the Eurasian vector of Russian development. In 1998, Sergey Rogov, Director of the Institute of U.S. and Canada at the Russian Academy of Science, articulated thoughts that had long been floating around in domestic political and intellectual circles.[49] The idea was to create a Eurasian Union, a special political, economic, and social entity, which would be attractive to all former Soviet states.[50]

In line with the newly articulated Eurasian aspirations, Moscow began to institute integration projects with FSU countries. In 1997, Russia signed the treaty on the Union State with Belarus,[51] along with the treaty on friendship, cooperation, and partnership with Ukraine.[52] In 2000, a treaty on the establishment of the Eurasian Economic Community was signed by Russia, Belarus, Kazakhstan, Kyrgyzstan, and Tajikistan.[53] In 2014, the organisation was replaced by the Eurasian Economic Union.[54]

After Vladimir Putin was elected President of the Russian Federation in 2000, he continued to reinforce the strengthening mechanisms of political and economic influence on

---

[49] Sergei Rogov, *A Eurasian Strategy for Russia* (Institute for US and Canadian Studies 1998).
[50] Teodor Lucian Moga and Denis Alexeev, 'Post-Soviet States Between Russia and the EU: Reviving Geopolitical Competition? A Dual Perspective' (2013) 13 Connections 41, 48.
[51] 'Treaty on the Union of Belarus and Russia' (*Official website of the Union State*, 1997) <http://www.soyuz.by/about/docs/dogovor3/> accessed 9 August 2019.
[52] Tsygankov (n 46) 285.
[53] 'Treaty on the Establishment of the Eurasian Economic Community' (*Eurasian Economic Community*, 2000) <http://www.evrazes.com/docs/view/95> accessed 9 August 2019.
[54] 'Treaty on the Eurasian Economic Union' (*Eurasian Economic Union*, 29 May 2014) <https://docs.eaeunion.org/en-us/Pages/DisplayDocument.aspx?s=bef9c798-3978-42f3-9ef2-d0fb3d53b75f&w=632c7868-4ee2-4b21-bc64-1995328e6ef3&l=540294ae-c3c9-4511-9bf8-aaf5d6e0d169&EntityID=3610> accessed 9 August 2019.

post-Soviet countries, and expanded the commanding presence within the region.[55] EU and NATO policies were interpreted as signs of political exclusion and as a direct threat to the national security of the Russian Federation.

3.2.2. Aftermath of the Colour Revolutions (Mid-2000s)

The second shift of the Russian Federation policies towards 'near abroad' countries occurred in the mid-2000s following the 'Colour Revolutions' in Georgia (2003), Ukraine (2004), and Kyrgyzstan (2005).[56] Russia more decisively articulated its desire to play a leadership role in the region, and its readiness to compete with Western countries in the territories of the former Soviet countries. During those years, Russia resorted to political pressure on its neighbours that expressed ambitions to cooperate with NATO and the EU, a reminder that this could lead to the withholding of economic and energy benefits.[57] At this stage, it became clear to the Kremlin that keeping and advancing its positions within the region would require stricter measures as well as a long-term strategy for the reintegration of former Soviet Republics.[58]

The favourable global conditions for the strong economic performance of the Russian Federation in the mid-2000s provided an enabling environment for its re-integration plans. As President Putin stated in 2006 at the meeting with Foreign Ministers of the FSU republics, the political powers in the world should be adopted in accordance with the newly opened economic opportunities.[59] In the meantime, establishing energy projects, such as the Nord

[55] Natalia Morozova, 'Geopolitics, Eurasianism and Russian Foreign Policy under Putin' (2009) 14 Geopolitics 667.
[56] Esmaeil Mazloomi, Emile Kok-Kheng Yeoh and Mohd Aminul Karim, 'From Status Inconsistency to Revisionism: Russian Foreign Policy after Color Revolutions' (2018) 19 Japanese Journal of Political Science 489.
[57] Moga and Alexeev (n 50) 47.
[58] ibid.
[59] Vladimir Putin, 'Vystupleniye na soveshchanii s poslami i postoyannymi predstavitelyami Rossiyskoy Federatsii [Speech During the Meeting with Ambassadors and Permanent Representatives of the Russian

Stream Pipeline, made Moscow less dependent on transit routes through Moldova, Ukraine, and Belarus to Western countries.[60] This gave Moscow a free hand to establish its own rules in Central and Eastern Europe.

3.2.3. Towards the New Cold War (Late 2000s)

The late 2000s marked the third shift, when Russia expressed the most articulate interest in a reversal of the fragmentation process in the post-Soviet territories following the downfall of the Soviet Union.[61] Competition between the EU and Russia for the region was elevated to the level of political and economic integration projects: the Eastern Partnership[62] *vis-à-vis* the Eurasian Economic Union.[63] Ideologically, the Russian Federation spared no resources when promoting its geopolitical idea of 'Eurasianism' with a centre of gravity in Moscow.[64]

The outright competition put Eastern European countries at a crossroads between Brussels and Moscow, and exposed them to pressure from both sides. This time Russia took a pragmatic approach in choosing integration stimuli – offering business benefits and opening new markets, which was very similar to the EU experience.[65] In particular, Russia initiated setting up the Eurasian Customs Union (2010), joined by Belarus and Kazakhstan. In 2001, eight CIS countries signed a free-trade agreement.[66]

Federation]' (*Official website of the President of Russian Federation*, 2006) <http://kremlin.ru/events/president/transcripts/23669> accessed 9 August 2019; Tsygankov (n 46) 285.

[60] Tsygankov (n 46) 285.

[61] Moga and Alexeev (n 50) 47.

[62] Ian Traynor, 'EU Pact Challenges Russian Influence in the East' *The Guardian* (7 May 2009) <https://www.theguardian.com/world/2009/may/07/russia-eu-europe-partnership-deal> accessed 9 August 2019.

[63] Andrei Skriba, 'Russian Strategy towards the Post-Soviet Space in Europe: Searching for Balance between Economy, Security, and Great Power Attractiveness' (2016) 40 Strategic Analysis 604, 606.

[64] Vladimer Papava, 'The Eurasianism of Russian Anti-Westernism and the Concept of "Central Caucaso-Asia"' (2013) 1 Ideology and Politics 68, 69–70.

[65] Moga and Alexeev (n 50) 47; Skriba (n 63) 606.

[66] 'Most CIS Countries Sign Up To Free-Trade Zone' (*RadioFreeEurope/RadioLiberty*) <https://www.rferl.org/a/cis_putin_free-trade_zone/24364420.html> accessed 12 September 2019.

The events in Georgia (2008) and Ukraine (2014) signalled that the Russian Federation was ready for an open confrontation in order to keep and expand its positions in the region. Already fraught with tension following the Georgian war, Russia's relationship with the EU and the US showed further signs of tension and deterioration after the invasion in Ukraine. Following the annexation of Crimea in March 2014, Canada, the US, and the EU introduced targeted economic sanctions to Russia,[67] which underwent several rounds of amendments in the following years. In April 2014, Russia was suspended from voting in the Parliamentary Assembly by the Council of Europe.[68] On July 2014, the EU expanded the list of sanctions against private individuals and entities.[69] The dialogue between Russia and Western countries was subdued or frozen altogether with regard to many bilateral concerns. Some experts interpreted these events as a manifestation of 'the new Cold War'.[70] Russian Prime Minister Dmitry Medvedev also suggested that tensions between Russia and the West could be equated to 'the new Cold War'.[71]

3.2.4. Frozen Conflicts and Unrecognised Territories in Post-Soviet Space

The events described below have often given impetus to practices curtailing freedom of expression online. This section is intended to cover the general background regarding frozen conflicts within the FSU, as the definitions, connection between the frozen conflicts,

[67] Council of the European Union, Council Decision concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine 2014 [2014/145/CFSP].
[68] Luke Harding, 'Russia Delegation Suspended from Council of Europe over Crimea' (2014) <https://www.theguardian.com/world/2014/apr/10/russia-suspended-council-europe-crimea-ukraine> accessed 12 September 2019.
[69] Council of the European Union, Council Implementing Regulation implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine 2014 [810/2014].
[70] Dmitri Trenin, 'Welcome to Cold War II' (*Foreign Policy*, 4 March 2014) <https://foreignpolicy.com/2014/03/04/welcome-to-cold-war-ii/> accessed 12 September 2019; 'Robert Legvold on the New Cold War, Interview with Columbia University Professor and Leading Russia Scholar' (*HuffPost*, 11 October 2015) <https://www.huffpost.com/entry/robert-legvold-on-the-new_b_8514120> accessed 12 September 2019.
[71] 'Russian PM Medvedev Says New Cold War Is On' *BBC News* (13 February 2016) <https://www.bbc.com/news/world-europe-35569094> accessed 12 September 2019.

and national security matters will be referred to in many additional parts of the analysis, notably in Section 6, *Post Soviet Region: Case Studies of Online Regulation.*

The downfall of the Soviet Union was experienced by its constitutive units in a number of different ways, at varying velocity and with diverse outcomes. It would be erroneous to present the fragmentation as a universal process across the entire set of ex-republics or smaller national entities. On the contrary, the disintegration proved to be a complex and messy overhaul involving diverse political, economic, social, and institutional dimensions with unique neighbours and borders, ethnic divisions, or national identities involved, and varying degrees of domestic instabilities or even conflicts. The restructuring called for leaders' and peoples' understanding of the new realities in the absence of the omnipresent ideological glue of state socialism, and a command and control ethos. In addition, conflicting 'East-West' messages reinforced fragmentation motives and strengthened centrifugal sentiments. Therefore, insecurities, divisions, and wounds − coupled with the omnipresent Russian interest − began to morph towards and resulted in a number of frozen conflicts and unrecognised territories.

The crises in Nagorno-Karabakh, Transnistria, Abkhazia, South Ossetia, and Donbas occurred owing to specific local processes and to Russian influence. Russia consistently used frozen conflicts as a lever of political pressure to force states to sign integration agreements with the RF or to deter Western influence on neighbouring states.

3.2.4.1. Nagorno-Karabakh

The dissolution of the Soviet Union provoked a dispute between Armenia and Azerbaijan over the Nagorno-Karabakh territory. This turned into the bloodiest conflict of the 1990s in post-Soviet space, resulting in the loss of approximately 25,000 lives.[72]

Russia provided both sides with weapons, although tending towards the pro-Armenian position. This was especially evident in the early stages of the conflict. After 1991, Armenia maintained close relations with Russia regarding national security, and agreed to the presence of Russian troops on its territory. Azerbaijan, however, refused to sign the CIS security pact in May 1992. As Betts notes, as a consequence, on the following day Armenia initiated a military assault, taking Nagorno-Karabakh under its own patronage. [73] The Russians did not provide military assistance to Azerbaijan until the country signed the agreement to join CIS in 1993.

The last time the Nagorno-Karabakh conflict escalated was in April 2016, which was considered the worst outbreak since the1994 ceasefire.[74]

The Armenian armed forces are fully reliant on support from the Russian Federation, and therefore, under the circumstances, the need for Moscow to influence Nagorno-Karabakh was almost disregarded. After the Armenian Velvet Revolution of 2018, the Russian press on one occasion portrayed the new Prime Minister Nikol Pashinyan as a 'carbon copy' of

[72] Arkady Moshes and András Rácz, 'What Has Remained of the USSR: Exploring the Erosion of the Post-Soviet Space' (Finnish Institute of International Affairs 2019) 58 54 <https://www.fiia.fi/wp-content/uploads/2019/02/fiia_report58_what_has_remained_of_the_ussr_web.pdf> accessed 12 September 2019.

[73] Wendy Betts, 'Third Party Mediation: An Obstacle to Peace in Nagorno Karabakh' (1999) 19 Sais Review 161, 177–178.

[74] 'Nagorno-Karabakh Clashes Kill Dozens' *BBC News* (3 April 2016) <https://www.bbc.com/news/world-europe-35949991> accessed 12 September 2019.

Ukrainian President Petro Poroshenko.[75] However, given the difficulties on the borders, it is most likely that maintaining a positive relationship with the Russian government will remain a significant strategic interest for any future Armenian leadership.[76]

3.2.4.2. Transnistria

During the interwar period of 1924-1940, Transnistria and Moldova constituted parts of two different countries. At that time, Transnistria was incorporated into the Ukrainian republic, and most of the other Moldavian lands were a part of Romania. The territories eventually reunited within the Soviet Union. The rise of nationalist and state-building ideas in Moldova in the late 1980s, the adopting of laws to promote Moldovan culture, [77] and debates about a possible reunification with Romania were viewed with fear and suspicion in Transnistria.[78] As a result of the 1989 revolution, Romania aligned itself with the West, whereas Transnistria remained a 'Russophone and industrialised'[79] region. Following the declaration of Moldavian SSR as a sovereign state, Transnistria announced its independence from Moldova.[80] However, the quasi-state never gained international recognition, with the latent conflict reaching a peak in March 2012. Unable to maintain control due to support by Russia and the 14th Army, the Moldovan military forces had to push back, and a ceasefire was signed in July 2012.[81] In the aftermath of the conflict, a joint peacekeeping force involving Moldova, Russia, and Transnistria is active in the region.

---

[75] Joshua Kucera, 'Russian Press Portrays Armenia's Pashinyan as "Carbon Copy" of Poroshenko' (*Eurasianet*, 23 July 2018) <https://eurasianet.org/russian-press-portrays-armenias-pashinyan-as-carbon-copy-of-poroshenko> accessed 12 September 2019.
[76] Moshes and Rácz (n 72) 77.
[77] Erika Dailey, Lois Whitman and Jeri Laber, *Human Rights in Moldova: The Turbulent Dniester* (Helsinki Watch 1993).
[78] Erik J Grossman, 'Russia's Frozen Conflicts and the Donbas' (2018) 48 Parameters 51, 53.
[79] Michael S Bobick, 'Separatism Redux: Crimea, Transnistria, and Eurasia's de Facto States' (2014) 30 Anthropology Today 3, 4.
[80] Dailey, Whitman and Laber (n 77) 13.
[81] Grossman (n 78) 53.

Although Russia did not recognise Transnistrian independence (alongside all UN states), Moscow is consistent in its military and financial support for separatists in the Transnistria Republic of Moldova. The Russian government is also taking steps regarding passportisation of the population: one in five Transnistrian citizens has a Russian passport, including the majority of the 'government'.[82] This situation created the pre-conditions for Russia to protect de-facto its citizens. Keeping this conflict unresolved and frozen, Russia's double purchase is to maintain leverage on Moldova's foreign policy. In the early 1990s, this advantage was played to integrate Moldova into the CIS,[83] while the Transnistrian issue now blocks Moldova from EU and NATO integration.[84]

3.2.4.3. Georgian Frozen Conflict: South Ossetia and Abkhazia

Unlike other frozen conflicts, the timeline of a series of disconnections in South Ossetia and Abkhazia can be divided into two parts. The first part began shortly before the downfall of the Soviet Union and lasted until 1992[85] in South Ossetia and 1994 in Abkhazia.[86] This period was associated with the rebirth of a national upsurge in society. Several legislative acts were passed to promote the Georgian language in public spheres of life and education specifically; in addition, an initiative was announced to establish the Georgian branch of Sukhimi University in Abkhazia.[87] These steps elicited serious concerns and tensions in South Ossetia and Abkhazia, the regions bordering the Russian Federation. They expressed their desire to be an autonomous part of the Soviet Union and Russia as its

[82] Bobick (n 79) 6.
[83] Helen Fedor, *Belarus and Moldova: Country Studies* (1st edn, Federal Research Division, Library of Congress 1995) 168.
[84] Grossman (n 78) 54.
[85] Dennis Sammut and Nikola Dvetkovski, *The Georgia-South Ossetia Conflict* (Verification Technology Information Centre 1996) 28.
[86] UN Security Council, Letter dated 17 May 1994 from the Permanent Representative of Georgia to the United Nations addressed to the President of the Security Council 1994 [S/1994/583].
[87] Sammut and Dvetkovski (n 85) 10.

successor.[88] The initial controversies and tensions in South Ossetia between state and separatist forces had already begun in 1989, and by 1991 they had resulted in an armed conflict. Unable to reverse USSR troop deployments to South Ossetia's capital, Tskhinvali, and facing a new separatist outbreak in Abkhazia, the Georgian government signed a ceasefire in 1992. It is difficult to measure accurately the role of Russia during the initial years of conflict, since it had started before the collapse of the Soviet Union. Therefore, the Russian mitigation of conflict in those early stages may be interpreted as a matter of internal security. Nonetheless, what should be noted is that the uprising of secessionist movements convinced the Georgian government to join the Commonwealth of Independent States.[89]

The second wave of conflict dates back to 2008, and became known as the Russian-Georgian War. After becoming an independent state, Georgia steadily supported the Western direction of development. In 2004, the country submitted a NATO Individual Partnership Action Plan. However, in 2008, at the NATO summit in Bucharest, its future membership in the organisation was assured through the granting of the Membership Action Plans to Georgia and Ukraine.[90] Georgian forces decided in August 2008 to return to controlling the frozen territories amidst a series of ongoing intense border skirmishes. Soon after, the Russian Government deployed armed forces to the region on the grounds of protecting the Russian minorities. This sizeable military support curbed Georgian efforts to regain control over these regions. The Russian-Georgian war lasted 5 days. As a result, Russia recognised the independence of South Ossetia and Abkhazia. Similar to the Moldavian scenario, Russia used the frozen conflict as an opportunity to prevent the neighbouring country from being integrated into western structures. Russia provided broad military, diplomatic, and economic

[88] Rachel Denber, *Bloodshed in the Caucasus: Violations of Humanitarian Law and Human Rights in the Georgia-South Ossetia Conflict* (Human Rights Watch 1992) 6–7.
[89] S Neil MacFarlane, 'On the Front Lines in the near Abroad: The CIS and the OSCE in Georgia's Civil Wars' (1997) 18 Third World Quarterly 509, 514.
[90] NATO, Bucharest Summit Declaration 2008.

assistance for this internationally unrecognised territory. According to the International Crisis Group, by 2010 Russia had invested 840 million US dollars in the territory; donated about 99 million US dollars to the local budget; and staffed the vast majority of the government.[91] In addition, Russia provided passportisation to people who lived in the region so that they officially became Russian citizens.[92]

3.2.4.4. Ukraine: Crimea and Donbas

The armed conflict in eastern Ukraine dates back to 2014, following the events of Euromaidan and the Russian annexation of Crimea. In February 2013, President Yanukovych refused to sign the EU-Ukraine Association Agreement, which had been on the table since 2007.[93] The brutal reaction of the regime to the first pro-EU meetings of students in Kyiv sparked a popular uprising known as Euromaidan or the Revolution of Dignity. As a result of these events, Viktor Yanukovych was ousted from the presidential post and left the country.[94]

Across the pro-Russian regions of Ukraine – Crimea, Lugansk, and Donetsk – Euromaidan events fostered a fear of the coming into power of a new ultra-nationalistic regime hostile to the ethnically Russian citizens, not least due to the Russian information-related efforts to frame Euromaidan as a 'fascist junta coup'.[95] Moscow was not going to allow the further integration of Ukraine into the EU and NATO, and such a scenario seemed very likely under the new pro-Western government.[96] At the end of February 2014, the local separatist forces in Crimea with the support of Russian military troops held a hasty

[91] 'South Ossetia: The Burden of Recognition' (International Crisis Group 2010) 205 i.
[92] Roy Allison, 'Russia Resurgent? Moscow's Campaign to "Coerce Georgia to Peace"' (2008) 84 International affairs 1145, 1147.
[93] Grossman (n 78) 57.
[94] ibid.
[95] Serhiy Kudelia, 'The Donbas Rift' (2017) 58 Russian Social Science Review 212, 219.
[96] Tsygankov (n 46) 287; Grossman (n 78) 57.

referendum (of dubious legitimacy) and annexed the peninsula.[97] Unlike in the other cases, Crimea cannot be considered a territory of frozen conflict, as the UN General Assembly did not recognise the results of the referendum and remained committed to the territorial integrity of Ukraine.[98] In a fashion similar to that involving the Crimean events, the local separatist forces and Russian 'volunteers' formed a militia in Donetsk and Lugansk.[99]

A significant factor in developments in the east of Ukraine appeared to be the political divide separating these territories from those of the majority of the country. The extent of the Donbas integration into the Ukrainian state was somewhat limited.[100] For instance, according to the survey undertaken in 2014, about 60% of the citizens in Donbas harboured regret regarding the disintegration of the Soviet Union, whereas in Ukraine about 33% of the citizens expressed that feeling.[101] The same study showed that 66% of the Donbas citizens had a sympathetic attitude towards Vladimir Putin, compared to the negative attitude of 76% of the population in other regions of Ukraine (the study was carried out after the annexation of Crimea). These facts lead to the conclusion that − while Russia effectively exploited the tensions around the Euromaidan events − the polarised public opinion within the country was also a factor.[102]

Eventually, the Donetsk and Luhansk regions proclaimed themselves to be independent republics. With Russian support, the militia was armed with sophisticated military equipment, which escalated the conflict to the level of 'tank battles and remote duels

[97] Alexei Anischchuk, 'Putin Admits Russian Forces Were Deployed to Crimea' *Reuters* (17 April 2014) <https://www.reuters.com/article/russia-putin-crimea-idUSL6N0N921H20140417> accessed 12 September 2019.
[98] UN General Assembly, Resolution adopted by the General Assembly: Territorial integrity of Ukraine 2014 [A/RES/68/262].
[99] Kudelia (n 95) 217.
[100] ibid 218.
[101] 'Nostal′hiya Za SRSR Ta Stavlennya Do Okremykh Postatey [Nostalgia for the USSR and the Attitude to Individual Figures]' (*Rating Group*, 2014) <http://ratinggroup.ua/research/ukraine/nostalgiya_po_sssr_i_otnoshenie_k_otdelnym_lichnostyam.html> accessed 12 September 2019.
[102] Kudelia (n 95) 212–221.

using rocket artillery'.[103] Considering this support,[104] at the end of summer 2014, Ukrainian military forces were compelled to switch from an offensive position to a defensive one.[105] Following Ukraine's defeat in the battle for Ilovaisk, and severe losses, Ukrainian leaders had to sign the Minsk Protocol[106] on a ceasefire through the Trilateral Contact Group − the group of representatives from Ukraine, Russia, and the OSCE − which facilitates the resolution of conflicts in the region.[107]

Compared to scenarios in Moldova and Georgia, in the case of Ukraine, Russia had to face much stronger resistance. Eventually, Ukraine received considerable political and military support from Western countries, which limited Moscow's capacities to dictate its own terms in resolving the conflict.[108]

The annexation of Crimea and the protracted armed conflict in Eastern Ukraine led Russia-EU relations to the breaking point. The Ukrainian developments appeared to be alarming for all CIS countries.[109] Even long-term Russian allies − for example, Belarus − emphasised their right to sovereignty and criticised the concept of a 'Russian World'.[110]

---

[103] ibid 226.
[104] Oksana Grytsenko, 'Thousands of Russian Soldiers Fought at Ilovaisk, around a Hundred Were Killed' (*KyivPost*, 6 April 2018) <https://www.kyivpost.com/thousands-russian-soldiers-fought-ilovaisk-around-hundred-killed> accessed 12 September 2019.
[105] Grossman (n 78) 58.
[106] 'Protocol on the Results of Consultations of the Trilateral Contact Group, Signed in Minsk, 5 September 2014' (*OSCE*, 2014) <https://www.osce.org/ru/home/123258> accessed 12 September 2019.
[107] 'Press Statement by the Trilateral Contact Group' (*OSCE*, 2014) <https://www.osce.org/home/123124> accessed 12 September 2019.
[108] Grossman (n 78) 59–60.
[109] Skriba (n 63) 613.
[110] 'Interv'yu Negosudarstvennym Sredstvam Massovoy Informatsii [Interview for Non-State Media]' (*Official website of the President of the Republic of Belarus*, 2015) <http://president.gov.by/ru/news_ru/view/intervjju-negosudarstvennym-sredstvam-massovoj-informatsii-11882/> accessed 12 September 2019.

3.2.5. Extremist Movements in the Post-Soviet Region

Amidst the dissolution of the Soviet Union, political instability gave rise to ethnic conflicts.[111] Economic and social gaps, in addition to ethnic divergence, created a hotbed for nationalism movements and discrimination between groups.[112]

Former Soviet republics inherited the same set of issues related to disputed boundaries, unclear identities, and a significant portion of the minority population.[113]

Many conflicts were concerned with territorial questions. Some nations required restoring boundaries that were changed during Soviet rule, others sought to renew territorial rights of forcefully relocated people.[114] Also, there were ethnic groups willing to reunite within one state.[115]

After the Soviet republics declared independence, smaller national groups within their territories also demanded sovereignty or special rights within the states.[116] The most violent conflicts were mentioned below in the section on frozen conflicts. Other examples include Chuvash, Udmurt, Tatarstan, Tuva, Komi-Permyak and other regions in Russia;[117] Samtskhe–Javakheti region in Georgia,[118] Gagauz region in Moldova.[119]

---

[111] Ian Bremmer, 'The Post-Soviet Nations after Independence' [2006] After Independence: Making and Protecting the Nation in Postcolonial and Postcommunist States 141, 142.
[112] Nadia Diuk and Adrian Karatnycky, *The Hidden Nations: The People Challenge the Soviet Union* (William Morrow & Co 1990) 47–71.
[113] Gail W Lapidus, 'Ethnic Conflict in the Former Soviet Union' (*CISAC*, 2005) <https://cisac.fsi.stanford.edu/research/ethnic_conflict_in_the_former_soviet_union/> accessed 13 March 2020.
[114] Airat Aklaev, 'Causes and Prevention of Ethnic Conflict: An Overview of Post-Soviet Russian-Language Literature' [2003] Leadership and Conflict Resolution: The International Leadership Series 249, 253.
[115] Aklaev (n 114).
[116] Bremmer (n 111) 142.
[117] Dmitry Gorenburg, 'Regional Separatism in Russia: Ethnic Mobilisation or Power Grab?' (1999) 51 Europe-Asia Studies 245; James Minahan, *The Former Soviet Union's Diverse Peoples: A Reference Sourcebook* (Abc-clio 2004) 312; Leokadia M Drobizheva, Rose Gottemoeller and Catherine McArdle Kelleher, *Ethnic Conflict in the Post-Soviet World: Case Studies and Analysis* (ME Sharpe 1998) 157–209; Aklaev (n 114).
[118] Justyna Mielnikiewicz, 'Post-Crimea, Phantom of Armenian Separatism Haunts Georgia' (*Eurasianet*, 2014) <https://eurasianet.org/post-crimea-phantom-of-armenian-separatism-haunts-georgia> accessed 13 March 2020.
[119] Steven D Roper, 'Regionalism in Moldova: The Case of Transnistria and Gagauzia' (2001) 11 Regional & Federal Studies 101.

Since the 1990s, the Chechen movement in the North Caucasus has shifted from being a nationalist agenda with the goal of achieving Chechnyan independence to that of embracing radical Islam.[120] After the Chechens' top commander, Dokku Umarov, proclaimed an Islamic state in the North Caucasus − the Caucasus Emirate − in October 2007, militants continued to attack Russians, developing a clear terrorist strategy and attacking civilians on the Russian mainland. The insurgents continued their activities even after the official end of the decade-long Second Chechen War in 2009.[121]

3.3. Interconnectedness of the Post-Soviet Region: Means and Narratives

A potential explanation for the cross-fertilisation of legal ideas across the FSU lies not only in the common socialist past but also in the fact that ties remain strong even up to the present. These ties exist across multiple dimensions, which will be presented in the following sections.

3.3.1. Means

3.3.1.1. Economic Ties

The transportation of oil and gas from Russia to Europe became a fundamental bargaining point of the Russian Federation's foreign policy, as Russia effectively employs the agenda of energy resources to maintain economic ties with post-Soviet Republics.[122] This creates strong leverage with regard to the countries traditionally dependent on the import of

[120] *See* Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries* (Hachette UK 2015) 246.
[121] *See* Cerwyn Moore, 'Foreign Bodies: Transnational Activism, the Insurgency in the North Caucasus and "Beyond"' (2015) 27 Terrorism and Political Violence 395, 406.
[122] Adam Fagan and Petr Kopecký, *The Routledge Handbook of East European Politics* (Routledge 2017) 364.

energy, such as Ukraine and Belarus.[123] For instance, with low energy prices, Belarus saved up to US$72 billion (€66 billion) from 2000 to 2015.[124]

As another economic benefit, Russia suggested opening its market to products from neighbouring countries that were striving to find a direction with regard to exporting their goods after the USSR's disintegration.[125] Moreover, Russia tended to support former Soviet states with loans. In exchange, the terms of such loans envisioned political loyalty rather than requests for reforms. Therefore, the arrangements proved much more attractive compared to IMF requirements.[126]

Against the backdrop of ongoing international cooperation between the EU and post-Soviet countries in the 2000s, the prices of oil and gas rose significantly. Moscow routinely exploited this factor in economic ties as a method of political pressure. By way of illustration, energy prices remained low provided that the purchasing country adopted favourable political decisions or agreed on the privatisation of factories by Russian businesses.[127] The latter model is illustrative of the economic cooperation between Russia and Belarus. If, however, a country was reluctant to accept the offer, it had to pay a higher price to import the energy; examples include Moldova, Georgia, and Ukraine.

Exploiting business connections worked for Russia business and politicians, successful in putting political pressure on countries where Russia has a strong economic footprint. In Latvia, for example, in recent decades businessmen who have financial interests

---

[123] Skriba (n 63) 608.
[124] Alexander Chubrik, *Russia: The Belarusian Challenge* (Carnegie Moscow Center 2016), cited in Skriba (n 63) 608.
[125] Commonwealth of Independent States, 'Free Trade Agreement between Azerbaijan, Armenia, Belarus, Georgia, Moldova, Kazakhstan, the Russian Federation, Ukraine, Uzbekistan, Tajikistan and the Kyrgyz Republic (Translation)' (*WIPO Lex*, 15 April 1994) <https://wipolex.wipo.int/en/text/228813> accessed 12 September 2019.
[126] Skriba (n 63) 608.
[127] ibid.

in Russia have achieved several leading government positions.[128] When Russian military forces entered Georgia, the Minister of Transport, Ainars Slesers, who had ties to Russian businesses, appealed to the Latvian National Assembly to consider the role of Georgia in provoking conflict.[129]

To spread its political influence, Russia takes advantage of opportunities involving European crises and weaknesses, starting with global financial crises, European predicaments such as Brexit, Eurozone crises, or the dramatic events in Syria or Ukraine. The agenda is focused on the 'collapse of the European economic and democratic system'.[130]

3.3.1.2. Military Ties

In a similar fashion, Moscow managed military cooperation between CIS countries. The Russian Federation positioned itself as a guardian of stability within FSU territory. In 1992, the Collective Security Treaty was signed by six CIS countries − Russia, Armenia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. Georgia, Azerbaijan, and Belarus adopted the treaty terms in 1994.[131] Members of the alliance declared they would not join any other military organisations or participate in military operations aimed at signatories of the Treaty.[132] In an event of external aggression that threatened the territorial integrity, stability, and sovereignty of any of the alliance members, other parties to the Treaty were obliged to provide military support. In 2002, the military alliance − the Collective Security Treaty

---

[128] Agnia Grigas, *Legacies, Coercion and Soft Power: Russian Influence in the Baltic States* (Chatham House London 2012); Heather A Conley and others, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Rowman & Littlefield 2016) 7.

[129] Alan McLean, Scott Shane and Archie Tse, 'Russia-Georgia Clash Worries Baltic States' (*NY Times Archive*, 15 August 2008) <https://archive.nytimes.com/www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html?_r=0#report/nato-08RIGA496> accessed 12 September 2019; Conley and others (n 116) 7.

[130] Conley and others (n 128) 5.

[131] European Parliament, 'At a Glance: Regional Organisations in the Post-Soviet Space' (2015) <http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/545718/EPRS_ATA(2015)545718_REV1_EN.pdf> accessed 12 September 2019.

[132] 'Collective Security Treaty' 1992.

Organisation (CSTO) − was established by six signatories, excluding Georgia, Azerbaijan, and Uzbekistan. In 2009, the signatory countries formed a collective military force.

However, a number of former Soviet Republics did not consider the CSTO to be an entirely beneficial organisation, and some parties refused to renew the Treaty in 1999. As their first move away from Russian influence, Georgia, Moldova, and Ukraine − the countries of particular strategic interest to Russia − chose not to enter into military cooperation with Russia. The ties in this area had weakened even more by the mid-2000s.[133]

The current CSTO members are represented by Russia, Belarus, Armenia, Kazakhstan, Kyrgyzstan, and Tajikistan.

The frozen conflicts within the post-Soviet territory played into Russia's hands in terms of stopping FSU countries from aligning themselves with NATO and its standards. Transnistria, Donbas, South Ossetia, and Abkhazia are reliant on Russian military support.[134]

3.3.1.3. Cyber Power and the Media

Mass media became a powerful tool in Moscow's domestic and foreign policy. Pro-Kremlin media outlets and 'troll factories' are commonly used to spread disinformation and Russian propaganda. For instance, the common narratives in the information war *vis-à-vis* the European Union embrace a range of discursive trends such as migration and economic issues, support of nationalistic views, the 2008 economic crisis, Brexit, and so on.[135] On the one hand, such actions are aimed at discrediting Russian opponents while justifying pro-Kremlin politics. On the other hand, the goal is to keep domestic electorates content with the Russian state's international image, and to assure the Russian population of the state's good reputation globally.

---

[133] Skriba (n 63) 609–610.

[134] See Section 3.2.4, '*Frozen conflicts and unrecognised territories in Post-Soviet space'.*

[135] Conley and others (n 128) 6.

An army of online trolls has infiltrated Internet space and social media platforms. These 'factories', whether human or automated, publish appropriately chosen pro-Kremlin comments on social media and in online media discussion threads,[136] and these have proven to be an effective measure to manipulate public opinion. The commentators commonly fabricate facts, and often spread fear among the audience.[137]

The Russian state-owned media have also spread propaganda messages to mobilise Russian compatriots in post-Soviet countries. The propagandistic media outlets, such as Russia Today and Sputnik, have opened new offices in a number of foreign countries, including the Baltic States, Eastern Europe, and the Balkans.[138]

In recent years, the Kremlin has managed to orchestrate a series of powerful cyber-attacks that have caused disruption and fear. The targets included, *inter alia,* governmental and non-governmental structures across the post-Soviet countries.

Ukraine, which experienced a growing number of cyber-attacks following the annexation of Crimea, could be a case in point. While the attention of the international community was focused on events in Donetsk and Lugansk, a string of Ukrainian organisations endured over 100 low-tech cyber-attacks. A few of these hacks were conducted using BlackEnergy malware, which is designed to gain control of computer networks.[139]

The Russian cyber-attacks also targeted financial institutions, although it remained unclear whether hackers sought to achieve financial or political gains. From 2013 to 2014, the

---

[136] Daisy Sindelar, 'The Kremlin's Troll Army' (*The Atlantic*, 12 August 2014) <https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/> accessed 12 September 2019.

[137] Aliya Sternstein, 'US Intelligence Community Keys in on the Russian "Troll Army" Manipulating Social Media' (*Nextgov.com*, 17 August 2015) <https://www.nextgov.com/cio-briefing/2015/08/us-intelligence-community-keys-russian-troll-army-manipulating-social-media/119158/> accessed 12 September 2019.

[138] Conley and others (n 128) 6.

[139] Owen Matthews, 'Russia's Greatest Weapon May Be Its Hackers' (*Newsweek*, 7 May 2015) <https://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html> accessed 12 September 2019.

attacks affected more than 100 banks in Ukraine, Europe, the US, and Japan. The heist is estimated to have totalled US$ 900 million (€822 million).[140]

3.3.1.4. Russian Orthodox Church

The Russian Orthodox Church plays an important ideological role in maintaining relations with neighbouring countries, and expresses unquestionable support of President Putin's political regime.[141] As Petro notes, the Church acts in partnership with the state rather than being subordinate to it.[142] The common ideological notions − for example, traditional family, the spiritual closeness with coreligionists, and the 'Russian World' ('Russki mir') values − are spread largely through church channels owing to the Church's influence.[143] The ROC serves as an advocate of these conservative values, as opposed to the liberal values proposed by the West.[144]

State officials and ROC leaders often share similar messages regarding neighbouring countries. By way of illustration, the leader of the Russian Orthodox Church, Patriarch Kirill, emphasised the spiritual unity of people living on the lands of Ancient Rus (currently Ukrainians, Russians, and Belarusians). According to his statements, the post-Soviet states constitute a wider ethnocultural entity.[145] Suslov noted that the principle of a 'Holy Russia', the postulated religious entity, which originated in Kievan Rus after Prince Vladimir baptised

---

[140] ibid.
[141] Nicolai N Petro, 'The Russian Orthodox Church' in Andrei P Tsygankov (ed), *Routledge handbook of Russian foreign policy* (Routledge 2018) 217–232.
[142] ibid 217.
[143] ibid 221–224.
[144] Mikhail Suslov, '"Russian World" Concept: Post-Soviet Geopolitical Ideology and the Logic of "Spheres of Influence"' (2018) 23 Geopolitics 330.
[145] 'Priyom po sluchayu tysyacheletiya prestavleniya svyatogo ravnoapostol'nogo knyazya Vladimira [Reception on the occasion of the millennium of Prince St. Vladimir Equal-to-the-Apostles]' (*Website of the President of Russia*) <http://kremlin.ru/events/president/news/50068> accessed 12 September 2019.

Kievan Rus in 988, is one of the dominant narratives embedded in the 'Russian World' vision.[146]

However, the impact of the ROC is not limited to the historical lands associated with Kievan Rus.[147]

The role of the Russian Orthodox Church in maintaining close connections with Russian compatriots abroad is often acknowledged by top governmental officials of the Russian Federation. Notably, at the ROC Bishops' Council of 2013, President Putin stressed that 'the Russian Orthodox Church has a special mission. It brings the nations and people together'.[148]

3.3.2. Narratives

3.3.2.1. 'Russian World' (Russkiy Mir)

According to Suslov, this Russian concept originated in the mid-1990s, and since then the term has undergone several notable shifts, particularly from an anti-territorial to a territorialised conception.[149] By and large, this principle refers to the idea that the 'geopolitical body of Russia is or should be bigger than Russia proper […] there is or should be some kind of legitimate political reasons'.[150] The last shift in the 'Russian world' imagery can be traced back to the 2010s, when the concept was articulated in a territorialised manner, and suggested an alternative to the Western model of modernity.[151]

---

[146] Suslov (n 144) 345.
[147] Petro (n 141) 225–226.
[148] 'Meeting with Bishops' Council members' (*Website of the President of Russia*) <http://kremlin.ru/events/president/news/17409> accessed 12 September 2019.
[149] Suslov (n 144).
[150] ibid 333.
[151] ibid 347.

According to Petro, both the state and the church have played a significant role in launching the 'Russkiy Mir' project.[152] From the Russian Orthodox Church perspective, 'Russkiy Mir' is neither a geographical nor an ethnic term, but is a spiritual entity shared by all Eastern Slavs and Orthodox coreligionists.[153]

From the state's perspective, the concept was adopted as an element of soft power and 'public relations initiative' to popularise Russia across post-Soviet states.[154] In recent years, the 'Russian World' concept has developed to the extent that it serves the ideological ground of annexations and Moscow's controversial politics.[155]

3.3.2.2. 'Saving Ethnic Minorities' (Russian Compatriots)

The Russian ethnic minorities or 'Russian compatriots' is another dimension embedded in the Russian foreign policy agenda. Given the considerable size of Russian diasporas across the former Soviet republics,[156] this fact, not surprisingly, has been used as a legitimate reason to expand Russian political influence far beyond the borders of the Russian Federation. Russia has claimed repeatedly that it could intervene in conflicts in the former Soviet Republics to protect the interests of ethnic Russians. This was a fundamental legitimising message during conflicts in Georgia[157] and Ukraine.[158]

On multiple occasions, the country's political establishment has stressed that the Russian Federation was obliged to protect the interests of all Russian compatriots abroad. Commenting on the annexation of Crimea, President Putin once noted that 'For me, it is not

[152] Petro (n 141) 217–232.
[153] ibid 221.
[154] ibid 222.
[155] Suslov (n 141) 347.
[156] ibid 331.
[157] Allison (n 92) 1153.
[158] Marlene Laruelle, 'Russia as a "Divided Nation," from Compatriots to Crimea: A Contribution to the Discussion on Nationalism and Foreign Policy' (2015) 62 Problems of Post-Communism 88, 95.

borders and state territories that matter, but people's [fates]'.[159] The Foreign Minister, Sergey Lavrov, justifying Moscow's decision to send armed troops to South Ossetia, stated that 'Russia will not allow the death of its compatriots to go unpunished'.[160] Moreover, these decisions garnered strong domestic public support. In 2014, 83% of the respondents in a public opinion poll agreed that the Russian Federation had to protect Russians residing in the Crimean peninsula even if relations with other countries worsened.[161] Of the respondents in an earlier survey in 2005, 93% agreed that the Russian Federation should protect Russians living abroad.[162]

3.4. Sub-Regional Groups in the Post-Soviet Region

Sub-regional peculiarities came to the fore during investigations of the legal initiatives across FSU. On the one hand, the Communist past resulted in a range of commonalities on Internet-regulation practices. On the other hand, each case requires historical contextualisation, as the region underwent diverse types of development following the collapse of the Soviet Union. For this reason, the author has included countries from various sub-regions in the analysis. This sub-section further explains the geographical delimitations of the present research project.

3.4.1. New Eastern Europe

The first group of countries lies on the border between the EU and the Russian Federation, and comprises Belarus, Moldova, and Ukraine.

---

[159] Nikolaus Blome and Kai Diekmann, 'For Me, It Is Not Borders That Matter' (*Bild*, 2016) <https://www.bild.de/politik/ausland/wladimir-putin/russian-president-vladimir-putin-the-interview-44092656.bild.html> accessed 12 September 2019.
[160] Allison (n 92) 1153.
[161] 'Krym i Rossiya: porozn' ili vmeste? [Crimea and Russia: apart or together?]' (*WCIOM*, 2014) <https://wciom.ru/index.php?id=236&uid=855> accessed 12 September 2019.
[162] John O'Loughlin and Paul F Talbot, 'Where in the World Is Russia? Geopolitical Perceptions and Preferences of Ordinary Russians' (2005) 46 Eurasian Geography and Economics 23, 42.

Geopolitically, those states are caught between the European Union and Russia.[163] Despite deep historical roots none of the states enjoyed independence up until 20th century, and thus they had a mild agreement on their national identity.[164]

Ukraine – with two brief former experiences of statehood – was caught between Eastern and Western agendas and respective historical and identity narratives.[165] Moldova – formed as a Soviet republic, confronted a separatist area that sought Russian integration against pro-Romanian citizens.[166] Prior to 1990s Belarus had no background as an independent country, and vague national identity.[167]

Following the dissolution of the Soviet Union, the position of newly established states was uncertain, and it was unclear whether they would be capable to manage as independent entities.[168] However, in recent decades the countries showed developments of nationhood in spite of various problems. Still, the future of New Eastern Europe remains highly reliant on dominant geopolitical powers represented by the EU and Russia.

As was noted above, these borderland countries were practically torn between 'the Wider Europe' and 'Eurasian' geopolitical courses.[169] In recent decades, they have lived through the fluidity of their governments' political 'multi-vector' ambitions. This region witnessed acute competition between Moscow and Brussels until it became so increasingly intense[170] that in 2014 it resulted in an armed conflict in Ukraine.

Even though the current situation in the region cannot be generalised – as countries are at various points of political and ideological spectrum – they possess many common

[163] Hamilton and Mangott (n 18) 1.
[164] ibid.
[165] Andrew Wilson, *The Ukrainians: Unexpected Nation* (Yale University Press 2015) 12–20.
[166] Charles King, *The Moldovans: Romania, Russia, and the Politics of Culture* (Hoover Press 2013) 1–11.
[167] Robert Legvold and Celeste A Wallander, *Swords and Sustenance: The Economics of Security in Belarus and Ukraine* (MIT Press 2004) 25–31.
[168] Hamilton and Mangott (n 18) 1.
[169] Fagan and Kopecký (n 122) 358–359.
[170] ibid.

features with other post-Soviet states. These include, for instance, distrust of state institutions, high level of corruption, strong links between political and business elites, the rule of political clans.[171]

The geopolitical vectors of these countries were different at various stages, and their loyalties to the Russian Federation diverged from country to country, they are akin on the basis of their objectives in building an independent statehood and becoming stronger as separate ethnic-cultural entities.[172] The Russian Federation's perception of these ambitions is a highly sensitive issue. The contradictions are probably weakest in Belarus, whereas in Moldova and Ukraine the ambivalence of the development vectors resulted in the frozen conflicts.[173] The countries have deep historical roots, and their connections can be traced back both to Russia and to the neighbouring Western states: Poland (for Ukraine) and Romania (for Moldova). In these countries, and over centuries, mutual interactions have affected the personal characteristics and attitudes of all the residents.[174]

The region constitutes a great geopolitical interest, because it is located on major energy, transportation and military routes between the Europe and Eurasia.[175] This is especially the case for Ukraine – due to the resources and the size, but also because it is a main country of transit of Russian gas to the EU.[176]

Moreover, due to proximity to the EU any security issues in the region – escalating of armed conflicts, organized crime, or viruses, – can have a spill over effect on the EU.[177]

---

[171] Hamilton and Mangott (n 18) 2.
[172] Fagan and Kopecký (n 122) 358–359.
[173] ibid.
[174] ibid.
[175] Hamilton and Mangott (n 18) 2.
[176] 'Russia, Ukraine Reach Five-Year Gas-Transit Deal' (*RadioFreeEurope/RadioLiberty*, 2019) <https://www.rferl.org/a/long-russia-ukraine-reach-five-year-gas-transit-deal/30353000.html> accessed 13 March 2020.
[177] Hamilton and Mangott (n 18) 2.

Oftentimes - because of the complex geopolitical position – experts described countries of the New Eastern Europe as "buffer states" between Russia and NATO. Chimiris described 'buffer zone' as a condition of confrontation between dominant powers when they enter the conflict on their periphery.[178] She suggested that examples of such dynamics might be observed both in Ukraine and Moldova. Thus, in Donbas region there are armed groups from neighbouring states. In Moldova, citizens make political decisions according to pro-Russian or pro-European backgrounds of politicians. Comparing to the neighbours, Belarus try to avoid 'zero-sum' game in relations with West and Russia. Instead, the country is trying to seek benefits on both sides.

The 'buffer zone' metaphor is not rarely applied in relation to new Eastern Europe. Makhovsky, for example, noted that the Kremlin 'sees Belarus as a buffer zone between the West and Moscow'.[179] Kosienkowski stressed that 'the maintenance of Moldova as a buffer zone only increased in importance with the 2004 NATO accession of Romania.'[180]

Walt and Mearsheimer noted that Ukraine remained a neutral buffer state at least up to the deposing of Yanukovych regime.[181] According to the authors, the lost of Ukraine's neutrality following the Euromaidan was among the key drivers of the confict in Donbas. As of now, Ukraine continues to pursue the policy towards the EU and NATO integration. In

[178] Ekaterina Chimiris, 'Eastern Partnership Countries: Buffer Zone or Platform for Dialogue?' (*Modern Diplomacy*, 13 November 2019) <https://moderndiplomacy.eu/2019/11/13/eastern-partnership-countries-buffer-zone-or-platform-for-dialogue/> accessed 11 March 2020.
[179] Andrei Makhovsky, 'Belarus Aims to Cut Russian Oil Supplies to 30-40% of Its Requirements: Belta' *Reuters* (21 January 2020) <https://www.reuters.com/article/us-belarus-oil-russia-diversification-idUSKBN1ZK1ED> accessed 11 March 2020.
[180] Marcin Kosienkowski and William Schreiber, *Moldova: Arena of International Influences* (Lexington Books 2012) 252.
[181] Stephen M Walt, 'History Shows Caution Is the Best Approach for Foreign Action' (*The New York Times*, May 2015) <https://www.nytimes.com/roomfordebate/2014/09/02/is-dont-do-stupid-stuff-the-best-foreign-policy-30/history-shows-caution-is-the-best-approach-for-foreign-action> accessed 11 March 2020; John J Mearsheimer, 'Getting Ukraine Wrong' *The New York Times* (13 March 2014) <https://www.nytimes.com/2014/03/14/opinion/getting-ukraine-wrong.html> accessed 11 March 2020.

2019, the Ukrainian Parliament voted to include this geopolitical choice to the Constitution.[182]

3.4.2. Baltic States

The Baltic States, represented by Latvia, Lithuania, and Estonia, became a part of the Russian Empire in the 18th century. During the interwar period of 1918-1940, however, these countries enjoyed independence, which sparked the restoration of national ideas. This process was brutally disrupted in 1940 when the Soviet Union incorporated the Baltic States under the Molotov-Ribbentrop pact.[183] The USSR continued to push its way towards the Baltic States at the end of WWII. The period up until the late 1950s saw the mass deportation of the Baltic population to Siberia, and, later, an inflow of Russian military to the region considerably transformed the political face of the countries.[184]

When the Baltic States restored their independence in the early 1990s, only Lithuania granted automatic citizenship to all permanent residents. Latvia and Estonia, having a large percentage of non-ethnic residents, required all residents to pass language and other tests in order to be granted citizenship. The status of Russian ethnic minorities up until the present remains a highly controversial topic of discussion between Moscow and the Baltic States.[185] For the sake of control over the Syrian refugee crisis in 2015, Latvia announced the building of a barbed wire fence on the border with Russia, and Estonia built a rampart. Once again, the Baltic States took on the role of 'cordon sanitaire', as had been done during the interwar periods.[186]

After Baltic States restored their independence, they took a consistent policy towards

[182] 'Ukraine President Signs Constitutional Amendment On NATO, EU Membership' (*RadioFreeEurope/RadioLiberty*) <https://www.rferl.org/a/ukraine-president-signs-constitutional-amendment-on-nato-eu-membership/29779430.html> accessed 11 March 2020.
[183] Fagan and Kopecký (n 122) 359–360.
[184] ibid.
[185] ibid.
[186] ibid.

European integration. Estonia, Latvia and Lithuania applied for EU and NATO membership in 2002, and all became members in 2004.[187] As of 2020, Baltic States are the only post-Soviet countries that joined both NATO and the EU.

Among all post-Soviet states the Baltic countries represent the most remarkable success story in terms of political, economical and legal reforms. As noted by Paulauskas, 'Baltic States managed to transform themselves from former Soviet republics with ruined economies and sovietized peoples into fully-fledged members of the EU with galloping economic growth and vibrant civil societies.'[188] In other words, the Baltic states now are fully integrated into EU legal architecture. This work will refer to an example of Estonia as a benchmark in terms of internet regulations.

3.4.3. South Caucasus

After the USSR dissolution the South Caucasus region, represented by Georgia, Armenia and Azerbaijan, got an opportunity to enter the global market.[189] In addition, they faced new geopolitical powers, since Turkey, Iran and the US challenged the Russian dominance of the last two centuries.

Geographically, the area can boast many critical factors such as natural wealth, e.g. gas and oil in the Caspian Sea; access to the Black Sea, regions of the Middle East and Central Asia.[190] Those resources made the region a subject of complex competition, not to mention internal issues such as the Nagorno-Karabakh conflict.

---

[187] 'Bush Welcomes New Nato Members' (*BBC*, 29 March 2004) <http://news.bbc.co.uk/2/hi/europe/3578837.stm> accessed 11 March 2020; 'EU Member Countries in Brief' (*European Union*, 16 June 2016) <https://europa.eu/european-union/about-eu/countries/member-countries_en> accessed 11 March 2020.

[188] Kestutis Paulauskas, *The Baltics: From Nation States to Member States* (European Union Institute for Security Studies 2006).

[189] Shafee (n 19).

[190] Stefan Georgescua, 'Geopolitical Changes in Caucasus After 1991' (2013) 3 Karabük Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 123.

In South Caucasus, the geopolitical agenda of the 1990s may be divided into external and internal factors. [191] Internal issues included ethnic conflicts, predicaments of transformation to a market economy and statehood development. Externally, the conditions were defined by joining the new players – Turkey, Iran, and Western countries, as well as the Russian attempts to maintain control over the region.

In the mid-2000s, a series of 'colour revolutions' on post-Soviet space shook the political situation in the region, and it seemed that the states would drift apart from Russia.[192] Nonetheless, since Russia strengthened its economic capacities, it returned to lading positions by 2008.

Georgia, Armenia, and Azerbaijan gained their independence following sensitive territorial conflicts, which exerted the greatest influence on their geopolitical choices.[193] These issues are described in detail in Section 3.2.4, which is devoted to the frozen conflicts. Russia continues to remain a strong player in the region, using the leverage of South Ossetian, Abkhazian, and Nagorno-Karabakh insecurities. Of all three states, Georgia has been the most consistent in paving its way towards integration with the EU and NATO. Armenia and Azerbaijan are long-term allies of Russia, primarily for the sake of their borders' security. The recent change of political leadership in Armenia has posed the question of whether cooperation with Russia will maintain the same dynamics. Given the complexity of the border, it is most likely that any future Armenian government will give special weight to the relationships with Russia.[194] Azerbaijan, enjoying oil resources and being a Caspian state, is more pragmatic and self-reliant with regard to any economic and military integration process.

---

[191] ibid; Shafee (n 19).
[192] Shafee (n 19).
[193] Moshes and Rácz (n 72) 77.
[194] ibid.

3.4.4. Central Asia

Whereas the countries of New Eastern Europe are torn by geopolitical vectors between the EU and/or Russia, the states of Central Asia are balanced between Russia and China. This sub-region comprises Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, and Turkmenistan. The post-Soviet era in these countries has perpetuated itself, as the long-term authoritarian regimes have persisted and have remained unchanged for decades.

The first President of Kazakhstan, Nursultan Nazarbayev, who served in the office for 29 years, was a major advocate of Eurasian integration. Thus, Kazakhstan became one of the founder states of EAEU. Nazarbatev's foreign policy approach displays the tendency to maintain a balance between the two superpowers represented by Russia and China.[195]

The former president of Uzbekistan, Islam Karimov, held the position for 27 years. He adopted the strategy of political isolationism, and did not position himself as a long-term and stable ally in any post-Soviet regional organisations. The country entered and then resigned from the Collective Security Treaty, GUAM, and CSTO.[196] However, the country underwent a change of political leadership, and the new president, Shavkat Mirziyoyev, has taken a much more open foreign policy direction than his predecessor.

Compared to its neighbours, Kyrgyzstan seems to be the least autocratic of the Central Asian states and the one most closely connected to China. Therefore, post-Soviet integration has looked promising for the political leadership of the country, which sought to counter-balance the Chinese impact.[197]

Because of its proximity to Afghanistan, Tajikistan was never of strategic interest to EAEU states, and EAEU membership was postponed by the member states due to security

[195] ibid 78–80.
[196] ibid.
[197] ibid.

risks. In turn, Tajikistan has been granted the leverage to estimate the cost of such an integration. The state is also considerably influenced by Iran, although the ethnic and linguistic ties do not guarantee a promising collaboration.[198]

Turkmenistan represents the harshest political regime within the region. Enjoying its generous reserves of natural resources, the country − in a manner similar to that of Azerbaijan − is in no rush to make any long-term international commitments.[199]

3.5. Evidence of Common Practices and Cross-Fertilisation

In recent years, legal scholars have expressed increased an interest regarding interaction between legal practices. In an international legal glossary, this trend was depicted by the term 'cross-fertilisation'.[200] Various examples may be found in the literature as regards usage of the term. According to Helfer, cross-fertilisation 'is one of the interpretative tools that are commonplace in the case law of regional and sub-regional [human rights] courts'.[201] Brown examines the interaction and common approaches between international judicial bodies, noting 'a significant level of cross-fertilization of principles among different international courts on various issues'.[202] Slaughter discusses transjudicial cross-fertilisation within the context of globalisation and establishing a global legal system.[203] According to the scholar, these two processes are interrelated.

It should be noted that international legal literature contains differential contextualisation of the term 'cross-fertilisation'. Scholars may refer to the concept when defining commonalities between court practices, but also in a broader sense − as any legal

[198] ibid.
[199] ibid.
[200] Ulf Linderfalk, 'Cross-Fertilisation in International Law' (2015) 84 Nordic Journal of International Law 428.
[201] Laurence R Helfer, 'The Successes and Challenges for the European Court, Seen from the Outside' (2014) 108 AJIL Unbound 74., cited in Linderfalk (n 200).
[202] Chester Brown, 'The Cross-Fertilization of Principles Relating to Procedure and Remedies in the Jurisprudence of International Courts and Tribunals' (2008) 30 Loy. LA Int'l & Comp. L. Rev. 219.
[203] Anne-Marie Slaughter, 'Judicial Globalization' (1999) 40 Va. J. Int'l L. 1103.

tool or technique borrowed from a foreign jurisdiction.[204] In this work, the author applies the term cross-fertilisation when denoting commonalities in legal frameworks – that is, national laws, strategic documents, court decisions, governmental directives, and so forth.

As to the regional groups under scrutiny, the evidence of cross-fertilisation may be found on many levels. Such cooperation is formed in the fertile ground of the common socialist past, and remains up to the present time in the form of regional organisations and multilateral and bilateral agreements. The cooperation is especially evident between similar political regimes – for instance, authoritarian governments draw inspiration from each other to stifle civil society and free speech.[205]

The commonalities exist on two levels: the actual wording of laws and regulations, as well as the continuity of the legal tradition. Cross-fertilization of laws in former Soviet republics is more complex than a repetition of laws: the countries have similar perceptions of the rule of law, unwritten practices, and relations between arms of government.

To set the stage, a deeper understanding is needed concerning the foundations behind contemporary legal systems in FSU. Scholars refer to several distinct features of the Soviet law.

Mälksoo mentions that 'Soviets argued the existence of a distinct 'Soviet' or 'socialist' international law' as the opposite of universal international law.[206] On the contrary, they asserted a separate regional agenda. Commonly, the USSR had its own 'flexible' interpretation of international law, while practical implementation of legal documents was completely different from what is declared on paper. For instance, the right to freedom of

[204] Linderfalk (n 200) 430.
[205] Adam Hug (ed), *Sharing Worst Practice: How Countries and Institutions in the Former Soviet Union Help Create Legal Tools of Repression* (Foreign Policy Centre 2016) 19–20.
[206] Lauri Mälksoo, *Russian Approaches to International Law* (Oxford University Press, USA 2015) 4.

expression, freedom of conscience was incorporated in Stalin's Constitution of 1936, even though those rights did not exist in practice.[207]

Galushko notes that 'though Stalin's constitution was proclaimed the most democratic in the world, 'the problem was that no one used it – neither Stalin nor the people'.[208] In other words, there was an evident disconnection between formal law, which oftentimes borrowed from the democratic Western tradition, and common law – a set of unwritten rules in society. Galushko calls this phenomenon a 'Two-Fold Constitutionalism'.

In Leninist ideology, the law held a special position. The aim of the legal system was not to serve as an independent body to ensure justice, but as an adjunct to the Communist party. [209]

The Soviet regime used the law as an instrument for show trials and fabrications. Pipes labelled this practice as 'legalized lawlessness'.[210] Such perception of legal order had a particular impact on popular attitudes toward law in society. The majority of the population saw law not as the supreme virtue but as a tool to ensure they individual conceptions about lawfulness and morals. [211] By way of illustration, Soviet citizens expressed little concern regarding legal procedures in the investigation of corrupt officials (with Brezhnev's son-in-law Churbanov).[212] In fact, the public did not question the use of Stalinist methods by investigators to get the admission of guilt from purported criminals.[213] The citizens expressed appreciation to the chief investigators – Nikolai Ivanov and Telman Gdlian – and elected

[207] ibid 6.
[208] Artem Galushko, 'Politically Motivated Justice in the Former Soviet Union: The Novel Concept of Two-Fold Constitutionalism in Post-Soviet States' (2016) 7 QMLJ 149, 152.
[209] Bohdan Vitvitsky, 'Why Is Raising the Level of Rule of Law In Post-Soviet Ukraine Such a Challenge?' (*VoxUkraine*, 16 September 2019) <https://voxukraine.org/en/why-is-raising-the-level-of-rule-of-law-in-post-soviet-ukraine-such-a-challenge/> accessed 8 March 2020.
[210] ibid.
[211] Peter H Solomon Jr, 'Gorbachev's Legal Revolution' (1990) 17 Can. Bus. LJ 184, 193.
[212] Michael Parks, 'Brezhnev Son-in-Law to Go on Trial in Corruption Case' (*Los Angeles Times*, 1 July 1988) <https://www.latimes.com/archives/la-xpm-1988-07-01-mn-6406-story.html> accessed 13 March 2020.
[213] Solomon Jr (n 211) 193.

them to the congress of Peoples' Deputies. At the same time, society did not perceive prosecutors and judges as officials who serve their best interests. The public had a low level of trust in law enforcement and judicial authorities and favored to keep away from them if possible.[214]

Officials in the Soviet Union commonly ignored the legislation. Sometimes they looked more carefully in regulations of government bodies than to the USSR laws. The same was applicable to law enforcement entities. Such neglect of legal norms created an atmosphere of 'legal nihilism' in society.[215]

Following the USSR dissolution – despite expectations of democratic reforms in former member republics – legal systems continued to operate in the same instrumental manner. The only difference was that except the Party it served the most powerful members of the national elite. [216]

Bader identified several reasons for the continuation of Soviet legal tradition.[217] First, in FSU elites had not fundamentally changed and were mainly formed from figures of former socialist rule. For instance, in Georgia, Azerbaijan, Uzbekistan and Kazakhstan election laws were drafted under presidents who were first secretaries of the republican organization of the Communist Party.[218]

Second, most of the post-Soviet countries did not have an independent statehood experience before the 1990s. Thus, they did not have the legal expertise to develop a

[214] ibid.
[215] ibid.
[216] Vitvitsky (n 209).
[217] Max Bader, 'The Legacy of Empire: A Genealogy of Post-Soviet Election Laws' (2012) 37 Review of Central and East European Law 449, 453.
[218] ibid.

qualitatively new legal system. Under these conditions, former USSR laws and new laws of the Russian Federation seemed like a feasible point of supply.[219]

Third, comparing to CEE states the FSU states had less interest from Western intergovernmental organizations e.g., OSCE or the Council of Europe or conceivable chances to join the European Union. Therefore, post-Soviet countries lacked incentives to reform legal systems in accordance with democratic standards.[220] At the same time, the majority of post-Soviet states continued to maintain relatively close ties with Russia – which the author pointed above in the section.

Last but not least, the leadership of post-Soviet states generally lacked the political will to reform political institutions. For instance, it appeared obvious in keeping the flawed election process in the region.[221]

Analysing the legal system in Ukraine in the early 1990s, Babie notes that the post-independent state retained the structure akin to the former Ukrainian Soviet Socialist Republic.[222] Despite the fact that many normative acts were adopted to consolidate Ukraine's independence and sovereignity, the new authorities were represented mainly by former communist officials. Thus, the elites were largely uninterested and incapable to implement meaningful reforms. The legal systems and institutions continued the general logic of the UkSSR. According to Lehman, that system was 'remarkably resistant to change.'[223]

As a main successor of the former Soviet Union, the Russian Federation plays a visible role across different sub-regional groups. There is 'a distinctively Russian tradition of thought and argument about human rights' that can be traced back to the imperial and Soviet

[219] ibid 454.
[220] ibid.
[221] ibid.
[222] Paul T Babie, 'Ukraine's Transition from Soviet to Post-Soviet Law: Property as a Lesson in Failed Regulation' [2016] U. of Adelaide Law Research Paper 9–10.
[223] ibid 10.

roots of the Russian Federation, and to the long history of serfdom in pre-Soviet Russia.[224] The particular traits of Russian legal thought arguably have spillover effects on countries that once shared the communist ideology with the Russian Federative Socialist Republic under the umbrella of the Soviet Union. Even decades after the collapse of the Soviet Union, the political, cultural,[225] and religious[226] ties with a number of Eastern European nations, as well as its strong position as an exporter of energy resources,[227] the Russian Federation still has a significant influence on Soviet successor states currently not in the EU − namely, Azerbaijan, Armenia, Belarus, Georgia, Moldova, and Ukraine[228] –

The commonalities in legal practices across the post-Soviet space can be illustrated fruitfully by the similar legislation limiting the activities of international NGOs, which have been negatively labelled 'foreign agents',[229] and by similar replications of the laws limiting 'unofficial public gatherings' as a tool to combat social protests. Moreover, within the CIS, cooperating countries draw up frameworks for the main regulatory documents – Civil Codes, Penal Codes, and so on.

By way of illustration, most of the CIS countries developed counter-terrorism policies based on the Model Statute 'On the fight against terrorism' from 8 December 1998 (the reworded version was adopted by the CIS Interparliamentary Assembly in 2004).[230] Under

---

[224] Bill Bowring, 'Russia and Human Rights: Incompatible Opposites' (2009) 1 Goettingen J. Int'l L. 257, 262.
[225] *See* Stefan Meister and Jana Puglierin, 'Perception and Exploitation: Russia's Non-Military Influence in Europe' (2015) 10 DGAP kompakt.
[226] *See* Daniel Washburn, 'Religious Tradition and Innovation in the Post-Soviet World: A Case of Revival of Rejection' (Cumberland Lodge 2007) <https://www.cumberlandlodge.ac.uk/sites/default/files/public/Religious%20Tradition%20and%20Innovation%20in%20a%20Post%20Soviet%20World.pdf> accessed 14 September 2019.
[227] *See* Ekaterina Demakova and Jakub M Godzimirski, 'Russian External Energy Strategy: Opportunities and Constraints', *Dynamics of energy governance in Europe and Russia* (Springer 2012) 150–151.
[228] *See, in general,* Joan DeBardeleben, 'The Impact of EU Enlargement on the EU-Russian Relationship' in Roger E Kanet (ed), *A Resurgent Russia and the West : The European Union, NATO and Beyond* (Republic of Letters 2009) 93.
[229] Hug (n 205) 19–24.
[230] Andrei Richter, *Post-Soviet Perspective on Censorship and Freedom of the Media* (UNESCO Moscow Office Moscow 2007) 232–233.

Article 21, the document provides for limitations with regard to reporting on terrorism-related matters, such as the restriction on disclosing details that might jeopardise counter-terrorism operations, or information on the personnel involved. This provision appears – in various forms – throughout anti-terrorism legislation in former Soviet republics, particularly in Belarusian and Ukrainian statutes.[231]

Max Bader undertook analysis of the election laws in 9 post-Soviet states: Uzbekistan, Tajikistan, Kazakhstan, Turkmenistan, Armenia, Kyrgyzstan, Belarus, Georgia, and Azerbaijan.[232] He noted, that electoral legislation in FSU states is not original, rather it borrows many provisions from Soviet and Russian laws. Particularly, 1988 and 1991 Soviet laws, the 1995 Russian laws on parliamentary and presidential elections, the 1997 general election law of Russia and the 1999 Russian law on parliamentary and presidential elections.[233]

As a result, the FSU states had a tendency to replicate laws of poor quality that allowed to held undemocratic elections and facilitated an 'authoritarian diffusion'.[234]

Bader stressed that 'diffusion' should not be confused with coercion, as most of the states voluntarily follow the Russian example. As for the reasons for 'diffusion', Bader brought the following points: 'the presence of one relatively hegemonic power in the region (Russia), a powerful common legacy (the Soviet Union), and a host of regional intergovernmental organizations.'[235] Apart from the election laws, he mentioned the adoption of comparable executive-legislative mechanisms, that emerged in the 1990s.

---

[231] ibid 233.
[232] Bader (n 217); Max Bader, 'Democracy Promotion and Authoritarian Diffusion: The Foreign Origins of Post-Soviet Election Laws' (2014) 66 Europe-Asia Studies 1350.
[233] Bader (n 217) 459.
[234] Bader (n 232) 1353.
[235] ibid.

In the late 1990s, Osakwe analysed the development of the first Russian and Kazakh Civil Code.[236] As for the Russian Civil Code, he stressed that it combined features of the Soviet legal tradition. This was understandable, since 'the drafters of the Code were themselves products of Soviet civil law and were deeply rooted in Soviet socialist legal tradition.'[237]

Osakwe named two documents 'ideological siblings', pointing out that they share many more features apart from the time of adoption.[238] In fact, the Kazakh Civil Code was almost identical to the Russian prototype. The differences were rather quantitative than qualitative.[239]

What added similarity to the Codes is that they borrowed from similar sources. One of the sources for drafts was the Model Civil Code for the CIS republics.[240] The Model Civil Code was taken by the Interparliamentary Assembly of CIS to guide member states in drafting their codes. In other words, it served as a 'skeleton' for legislators to construct own civil codes. Due to the Model Civil Codes, respective codes in CIS countries share common features in terms of 'structure, content, and philosophy'.[241]

Yunusov studied the development of legal systems in Central Asian states, and the adoption of Civil, Criminal Codes and other normative acts.[242] He noted, that new legal systems included many international norms in line with Roman-Germanic traditions. However, the legislation kept the logic and structure of Soviet legal tradition and remained

[236] Christopher Osakwe, 'Anatomy of the 1994 Civil Codes of Russia and Kazakstan: A Biopsy of the Economic Constitutions of Two Post-Soviet Republics' (1997) 73 Notre Dame L. Rev. 1413.
[237] ibid 1425.
[238] ibid 1414.
[239] ibid 1419.
[240] ibid 1426–1427.
[241] ibid.
[242] Khaydarali Yunusov, 'The Development of Legal Systems of Central Asian States' [2014] Studii Europene 23, 2.

coherent with the CIS legal space. Most of the Codes are similar to the respective codes in the Russian Federation.[243]

Apart from normative acts, commonalities are also evident in the judicial system. Elsuwege, for example, noted that except Turkmenistan, all constitutional courts in the post-Soviet area were modeled on the Russian Constitutional Courts.[244]

Galushko pointed out the similarities of unwritten judicial practices in post-Soviet space. [245] By analysing the cases of politicized criminal justice in FSU specifically represented by trials against the opposition, he noted that in many former Soviet republics the constitutional norms are present on paper only. In this way, the states continue the tradition of 'Two-Fold Constitutionalism' of the former Soviet Union – a set of unwritten norms that supercede the formal law. The latter practices include accusation bias, ex parte communication, judicial prerogativism, forced confessions, and political amnesties.[246]

[243] ibid.
[244] Peter Van Elsuwege, 'The Law and Politics of Post-Soviet Constitutionalism' [2019] What has remained of the USSR. Exploring the erosion of the Post-Soviet Space 21, 34.
[245] Galushko (n 208).
[246] ibid 153–160.

4. Expression Online and National Security: Concepts and Definitions

Barak sees balancing as 'a metaphor, which assumes the shape of a scale' on one side of which are the goals to be achieved, while on the other side are the limitations on rights.[247] This section provides a definition of the key terms used in the analysis, as well as the main principles regarding the balancing between freedom of expression online and national security.

4.1. National Security: Traditional Approaches

The concept of national security has long-term historical roots as old as the nation states themselves, whereas the term has only fairly recently originated in the English language.[248] Cameron suggests that the term became commonly used from the beginning of the Cold War, and the 1947 US National Security Act was among the first statutes to include the term.[249] Prior to this date, the United States commonly applied the term 'national defence', and the United Kingdom referred to the 'defence of the realm'.[250] National security in fact encompasses various linguistic and functional contexts; however, due to the constraints of the present study, the author will refer to the understanding of the term in international and domestic law. In this regard, Cameron draws attention to several pivotal principles.[251]

---

[247] Aharon Barak, 'Proportionality and Principled Balancing' (2010) 4 Law & Ethics of Human Rights 1.
[248] The 'term' and the 'concept' have different meanings. The term – is a particular phrase that refers to the concept. For instance, the terms − e. g. 'national security', 'state security', and 'defence of the state' − are all related to the concept of 'national security'. See Iain Cameron, *National Security and the European Convention on Human Rights* (Martinus Nijhoff Publishers 2000) 39.
[249] Cameron (n 248).
[250] ibid.
[251] ibid 40–49.

Firstly, the term 'national security' is not equal to that of 'national safety'.[252] The former implies a certain degree of severity regarding a threat *vis-à-vis* a state, up to the risk of national eradication.[253] Moreover, the security provisions – as they are indicated as 'national' – concern all citizens rather than prioritised social groups, particularly with respect to weakened governmental regimes that declare their own interests as being in line with those of the nation.[254]

Secondly, the age of global interconnectedness comes with adjustments to the implications of national security.[255] Therefore, national security extends not only to the protection of territorial integrity and combating external military attacks[256] but also includes the possibilities of economic and political espionage, the disturbing interference of foreign powers, terrorism, and cyber-attacks. Furthermore, internal challenges, such as ethnic conflicts and the violent overthrow of the established political order, should be taken into account. Clearly, the majority of governments address the latter as legitimate security issues.[257] Chandra and Bhonsle provided a valuable analytical overview as to the complexities of national security with respect to globalisation.[258] They emphasised that the concept should be viewed in a holistic manner, since 'there is no facet of national life that

[252] ibid 42.

[253] Cameron (ibid.) mentions, *inter alia*, 'Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' (The American Association for the International Commission of Jurists 1985) <https://www.icj.org/siracusa-principles-on-the-limitation-and-derogation-provisions-in-the-international-covenant-on-civil-and-political-rights/>. Principle 30 rules that 'National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order.'

[254] Barry Buzan, *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Harvester Wheatsheaf 1991); Cameron (n 248) 43.

[255] Satish Chandra and Rahul Bhonsle, 'National Security: Concept, Measurement and Management' (2015) 39 Strategic Analysis 337.

[256] See 'Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' (n 253). Principle 29 suggests that 'National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force'.

[257] Cameron (n 248) 43.

[258] Chandra and Bhonsle (n 255).

does not impinge on national security'. Whereas *ab initio* the issues such as ecology, individual well-being, and liberties seem distant from the objectives of national security, a closer inspection reveals their interconnectedness.

In social sciences – namely, in in the area of international relations − national security is commonly understood as a set of external and internal policy goals aimed at preventing states from becoming vulnerable.[259] According to this approach, national security is a goal of the governmental policy to create foreign and domestic political conditions that protect *national values* from the state's enemies.[260] This universal perception enables the collation regarding various state security policies. Nonetheless, the particular components of national security are still undefined and subjective in terms of the above concept, as each state determines individually and prioritises its core values, threats, and security priorities.[261] It may be suggested that the components are dictated by the geopolitical position of the state, by different political and military challenges, by economic conditions, and by development of the public institution, and so on.[262]

In turn, the 'threats' – under the suggested definition – may involve a long list of issues, starting with armed interventions, but also anything perceived by the state as a 'value'. By way of illustration, states with a long liberal and democratic tradition can invoke the protection of human rights a fundamental 'value' and a national security matter.[263] Obviously, the stability of bordering countries may be a subject of national security.[264]

---

[259] Buzan (n 254).
[260] Jorge A Tapia-Valdes, 'A Typology of National Security Policies' (1982) 9 Yale J. World Pub. Ord. 10, 11.
[261] Barry Buzan, *People, States, and Fear: The National Security Problem in International Relations* (Wheatsheaf Books Brighton 1983) 44–53.
[262] Cameron (n 248) 44; Buzan (n 254).
[263] Ramses A Wessel, *The European Union's Foreign and Security Policy: A Legal Institutional Perspective*, vol 33 (Martinus Nijhoff Publishers 1999) 68.
[264] Cameron (n 248) 44.

State sovereignty is one of the major notions with respect to national security. Sovereignty implies the full and sole right and power of the state, as an independent governing body, to make decisions with regard to its borders.[265] Any inference from outside actors is considered to be harmful to the state's sovereignty. The era of globalisation may be challenging for the sovereignty, however, with some scholars perceiving an extremely negative interconnection between these two components as states lose their power in terms of autonomous regulation of the economy, public goods, and so forth.[266] The states of course are constantly upgrading legal frameworks and control mechanisms in tandem with global threats.

Moreover, Cameron contextualises national security in terms of domestic and international law. As for domestic law, it is useful to distinguish between normative propositions and descriptive legal instruments.[267] Normative propositions are the statements employed in legal rules, and they do not evaluate actions. The descriptive provisions contain an evaluation of an action, and may be challenged to be true or false. Furthermore, propositions cannot be perceived as being the same in both international and domestic law.[268] For instance, 'state' would not have the same meaning in the international or domestic legal system. From the perspective of international law, the state is an actor that interacts with equal entities through 'horizontal' power relations. In contrast, at the domestic level, interactions between the citizens and the state originate in the 'vertical' dimension. Therefore, domestic law regarding national security usually implies constitutional, statutory, and other legal instruments for implementing state power with regard to citizens. In turn, state power is

[265] Stephen D Krasner, *Problematic Sovereignty: Contested Rules and Political Possibilities* (Columbia University Press 2001) 5–7.
[266] Christian Fjäder, 'The Nation-State, National Security and Resilience in the Age of Globalisation' (2014) 2 Resilience 114.
[267] Åke Frändberg, 'An Essay on the Systematics of Legal Concepts' (1987) 31 Scandinavian Studies in Law 81, 85., cited in Cameron (n 248) 45.
[268] Cameron (n 248) 45.

partitioned between executive, legislative, and judicial branches. For that reason, referencing national security is not only a matter of state power against individuals but is also a matter of power relations between governmental branches.

At the international as well as the domestic level, national security commonly serves as justification for certain categories of action that would be, in any other case, forbidden under international law;[269] for instance, the customary international law rules against the use of force except in the case of self-defence.[270] Whereas Article 2 of the UN Charter[271] rules that Members 'shall refrain … from the threat or use of force against the territorial integrity or political independence of any state', Article 51 recognises the right 'of individual and collective self-defence if an armed attack occurs against a Member'.

Treaty regimes provide valuable contextualisation with respect to the use of national security in international law. National security provisions may be excluded from the treaty, or serve as a condition for non-compliance or abandoning the international agreement.[272] This is exemplified by Article 26 Vienna Convention on Diplomatic Relations,[273] which rules that foreign diplomats may be prohibited from entering certain territories on the basis of national security concerns. The Convention on the Law of the Sea, in Article 19.2, stipulates that foreign ships posing a threat or using force against the territorial integrity of the coastal state fall outside any protection that would guarantee safe passage through territorial waters.[274]

International human rights conventions are yet another group of treaties, where exceptions on national security grounds become evident. In particular, in the European

[269] ibid 46.
[270] International Court of Justice, Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons 1996.
[271] United Nations, Charter of the United Nations 1945 [1 UNTS XVI].
[272] Cameron (n 248) 47.
[273] Vienna Convention on Diplomatic Relations 1961 [500 UNTS 95].
[274] United Nations Convention on the Law of the Sea (UNCLOS) 1982 [1833 UNTS 3; 21 ILM 1261].

Convention on Human Rights,[275] the exceptions with relation to national security are envisaged in the following:

- Article 6 on a right to a fair trial (judgements are to be pronounced publicly, but media and the public can be excluded on the basis of national security concerns);
- Article 8 on a right to respect for private and family life;
- Article 10 on freedom of expression;
- Article 11 on freedom of assembly and association.[276]

As already noted in this section, the categories that are defined as valuable for state protection have a major impact on the context of national security. For instance, the wording of the Convention introduces a long list of associated terms in line with national security: for example, 'public order', 'public safety', 'territorial integrity', 'economic well-being', 'protection of health and morals', and 'protection of freedoms of others'. Article 15 stipulates that the parties may derogate from the provisions of the treaty in the event of 'war or public emergency threatening the life of a nation'.

In the American Convention on Human Rights,[277] 'national security', 'public order', 'public health and morals', and 'rights and freedoms of others' are subjects of protection that may justify limitations, *inter alia*, to the rights of freedom of thought and expression, assembly, freedom of association, and freedom of movements and residence. Under Article 27 of the treaty, parties may derogate from treaty obligations in the event of 'war, public danger, or other emergency that threatens the independence or security'.

[275] European Convention on Human Rights 1950.
[276] For limitations to Articles 8-11, see, in general, Steven C Greer, *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, vol 88 (Council of Europe 1997).
[277] American Convention on Human Rights 1969 [1144 UNTS 123].

Additionally, military treaties may shed some light on the concept of national security. The principles of the North Atlantic Treaty[278] declare democracy, liberties, and the rule of law, peace, and security as core values to be defended by signatories. Article 5 contains a principle of 'collective defence': that is, if one of the parties is attacked, the other parties shall perceive this threat as an attack on their own state. The North Atlantic Treaty Organisation, under the 2010 Strategic Concept, designated collective defence as a core task along with crisis management and collective security. The organisation's strategic view encompasses the current challenges in international security, such as terrorism, cyber attacks, and the proliferation of nuclear weapons.[279]

In the view of the Organisation for Security and Co-operation in Europe – the world's largest intergovernmental security organisation – the notion of security touches upon many aspects of daily lives within politico-military, human, economic, and environmental dimensions. The list of security-related matters includes, *inter alia*, environmental issues, gender equality, media freedom, minority rights, and democratisation.[280]

The wording and applications of 'national security' in international treaties have multiple variations. In a manner similar to that involving a domestic level, the concept would depend on decision-holding persons and entities. Whereas the supervisory body responsible for implementing the agreement is not established, the power is divided equally between the treaties. For this reason, the governments referring to national security clauses will generally

[278] NATO, The North Atlantic Treaty 1949 [34 UNTS 243].
[279] 'Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization' (19 November 2010) <https://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf> accessed 8 July 2019.
[280] 'Factsheet: What Is the OSCE?' (*OSCE*, 11 July 2019) <https://www.osce.org/whatistheosce/factsheet> accessed 7 August 2019.

be able 'to spin this' to their advantage, except in cases of extreme resistance from other contracting parties.[281]

4.2. Terrorism: In Search of a Definition

National security issues arising from terrorism and violent extremism activities seem to be the most crucial on federal and global levels in recent years, especially following the 9/11 attacks.[282] Prior to analysing the role of the Internet in terrorism-related activities, the overall complexity of defining 'terrorism', 'extremism', and other key terms should be noted.

Whereas terrorism is an older concept dating back to the 19th century,[283] to date there is no universally agreed definition of the phenomenon. The absence of a standard legal definition adds complexity, making it difficult for states to develop regulations on national security, including those online. As the Lebanese President, Emile Lahoud, pointed out during a meeting of diplomats in 2004, 'It is not enough to declare war on what one deems terrorism without giving a precise and exact definition'.[284] Defining terrorism is often problematic, because the term is politicised, and is being used as a way of stigmatising objectionable political groups.[285] Therefore, most of the suggested definitions fail to address terrorism with the precision required in international law.[286]

---

[281] Cameron (n 248) 48–49.

[282] Following the terrorist attacks of September 2011 in the United States, a global 'war on terrorism' was declared. See Cynthia C Combs, *Terrorism in the Twenty-First Century* (Routledge 2017) 2; Christian Walter, 'Defining Terrorism in National and International Law' (2004) 1 Terrorism as a Challenge for national and international Law: Security versus Liberty 24, 2.

[283] David Rapoport defines 'four waves of terrorism': 'anarchist' (1880s-1920s), 'anti-colonial' (1920s-1960s), 'the left wing' (1960s-1990s), 'religious' (present time). See David C Rapoport, 'The Four Waves of Rebel Terror and September' (2002) 8 Anthropoetics.

[284] 'Beirut Wants "terrorism" Defined' (*Aljazeera*, 13 January 2004) <https://www.aljazeera.com/archive/2004/01/200841010738460226.html> accessed 18 July 2019.

[285] Combs (n 282) 2; Walter (n 282) 22.

[286] Combs (n 282) 3.

Nonetheless, up until now the definitions used in international customary law and national legal practices have shown some agreement on the key elements of terrorism. Taking these components together, Combs defined terrorism as a:

> *synthesis of war and theater, a dramatization of the most proscribed kind of violence − that which is deliberately perpetrated on civilian non-combatant victims − played before an audience in the hope of creating a mood of fear, for political purposes*.[287]

In broad terms, terrorism encompasses a violent action, an act committed with a certain level of cruelty. In addition, terrorist attacks imply the intention of creating fear and panic in society. The most common objectives − include religious and ideological − are related to political or social motives. As for the targets, the attacks generally affect non-combatant civilian victims. In other words, terrorists do not search for particular individuals in order to perpetrate violent actions − it is usually third parties who suffer, who are simply casualties, in order for terrorists to reach their objectives.[288]

It should be noted that a specific definition does not necessarily include all the aforementioned categories. However, certain elements would be incorporated into the term, establishing the concept of a terrorism rubric.

As illustration, the understanding of terrorism in the UK Terrorism Act 2000 implies, *inter alia*, an action that 'involves serious violence against a person', a threat that is created to influence the government or to 'intimidate the public', 'for the purpose of advancing a political, religious, racial or ideological cause'.[289]

---

[287] ibid 5.
[288] ibid 6.
[289] Terrorism Act 2000 2000 [2000 c. 11].

The U.S. Department of Defence defines terrorism as 'the unlawful use, or threatened use, of force or violence against individuals or property to coerce and intimidate governments or societies, often to achieve political, religious, or ideological objectives'.[290]

NATO defines terrorism as:

> *the unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives*.[291]

On 16 February 2011, the Special Tribunal for Lebanon issued a judgement regarding a customary definition of terrorism, which relied greatly on the aforementioned categories. In the view of the Tribunal, various treaties, UN resolutions, and national legislative practices provided grounds to define common *opinio juris* on international terrorism, particularly in a time of peace. Therefore, Paragraph 85 suggested that international terrorism has the following characteristics:

> *(i) the perpetration of a criminal act (such as murder, kidnapping, hostage-taking, arson, and so on), or threatening such an act; (ii) the intent to spread fear among the population (which would generally entail the creation of public danger), or directly or indirectly coerce a national or international authority to take some*

---

[290] *Military Operations in Low Intensity Conflict. Field Manual 100-20/Air Force Pamphlet 3-20* (Headquarters, Department of the Army and the Air Force 1990) 3–1.

[291] NATO Standartization Office, *AAP-06 NATO Glossary of Terms and Definitions* (2018th edn, NATO Standartization Office 2018).

> *action, or to refrain from taking it; and (iii) when the act involves a transnational element*.[292]

The above definition resulted in heated discussions, and was not widely recognised. Experts noted that the ruling failed to meet the required legal threshold with respect to national legal applications and *opinio juris*.[293] According to Saul, although the judgement relied on state practices as a part of the argumentation, it actually proved the absence of an agreement on a universal definition of terrorism. Nonetheless, the Tribunal decision demonstrated that the definition of terrorism in customary law is likely to evolve.[294]

Within the United Nations, debates on a universally agreed definition of terrorism have been going on since at least the late 1990s.[295] One of the major documents was a Draft Comprehensive Convention on International Terrorism,[296] which suggests that terrorism is an offence causing: a) death or serious bodily injury to any person; or b) serious damage to a State or government facility, a public transportation system, communication, or infrastructure facility. The clause specifies that the actions mentioned are committed intentionally, with a view to 'intimidate the population' or to influence the politics of governments and international organisations.

Analysing national and international terrorism legislation, Walter divided objective and subjective elements in the existing definitions.[297] The objective element refers to

---

[292] *Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging* [2011] Special Tribunal for Lebanon STL-11-01/1. For details of the decision, see, in general, Prakash Puchooa, 'Defining Terrorism at the Special Tribunal for Lebanon' [2011] Journal of Terrorism Research.

[293] 'Education for Justice University Module Series. Defining Terrorism.' (*UNODC*, July 2018) <https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html> accessed 8 August 2019.

[294] ibid.

[295] ibid.

[296] The draft treaty was proposed by India during the UN General Assembly in 2000. See UN General Assembly, Measures to eliminate international terrorism (Report of the Working Group) [C.6/55/L.2] Annex II.

[297] Walter (n 282).

committing a certain criminal act, usually violence against other individuals.[298] Nevertheless, the serious damage to public property, or to infrastructure facilities of crucial importance, may also be considered an act of terrorism. The latter provision was included, *inter alia*, in Canadian Bill C-36,[299] the UK Terrorism Act 2000,[300] and the Framework Decision of the Council of the European Union.[301]

The subjective element, in turn, encompasses the intent to create a climate of fear and terror within a population, or declaring threats of committing an attack. Many modern definitions incorporate religious, political, or ideological motives behind terrorist acts as the defining characteristics that differentiate them from other criminal activities.[302] However, it is not always the case, and some broader definitions do not take into account the motives behind attacks. It is exemplified in the EU Framework Decision,[303] which proffers a long list of activities as possible terrorist offences, including 'attacks on the physical integrity of a person', 'kidnapping and hostage', and the 'seizure of aircraft', but in the meantime does not require such actions to be politically or ideologically motivated.

The lack of a universal definition of terrorism in the legal area raises various issues. To begin with, the lack of the term encourages its politicisation. Therefore, a number of non-terrorist (or even non-criminal) actions could be defined falsely as terrorism-related offences.[304] Such a risk is primarily unfair with regard to countries having a poor environment involving human rights. The other effect is an inconsistency at both national and

[298] Cf. ibid 5–6; Combs (n 282) 6–10.
[299] Government Bill (Anti-terrorism Act) 2001 [C-36 (37–1)].
[300] Terrorism Act 2000 (n 289) s I.
[301] Directive (EU) of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA 2017 [2017/541].
[302] Cf. Walter (n 282) 6–9; Combs (n 282) 6–12.
[303] Directive (EU) of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (n 301) Art. 3.
[304] 'Education for Justice University Module Series. Defining Terrorism.' (n 293).

international legislative levels. Although intergovernmental organisations declare 'global war' on terrorism, and encourage states to adopt efficient national laws, the lack of a common term results in an absence of harmonisation involving legal action.[305] This absence is more likely to impede than to strengthen global cooperation.

4.3. Extremism and Radicalisation

Terrorism is linked closely with two other security challenges: violent extremism and radicalisation. Like terrorism, extremism and radicalisation to date have no comprehensive definition.[306] As a result, the three different phenomena are commonly attributed the same meaning, which hinders the efforts in combating violence. Moreover, the problem of definition is exacerbated by political speculations and social labelling with respect to extremism and radicalisation. These activities are perceived as 'terrorism' by default; however, this is not necessarily the case.[307] The other issue is that extremist ideologies might be falsely attributed to certain nationalities or religions, although the risks are by no means ethnically or geographically limited.[308]

A recent study by Striegher[309] provided a useful comparison of the terms. Whereas radicalisation is a process of individual transformation towards an extreme ideology, extremism is itself an ideology that promotes the use of violence in the interests of politics or religion. Terrorism, in turn, is a violent criminal act. Indeed, in some cases all the actions mentioned are links in a chain, in the sense that radicalisation leads to commitment to extremism and to the readiness to carry out a terrorist attack. In practice, however, the

---

[305] ibid.

[306] 'Education for Justice University Module Series: Radicalization & Violent Extremism' (*UNODC*, July 2018) <https://www.unodc.org/e4j/en/terrorism/module-2/key-issues/radicalization-violent-extremism.html> accessed 11 August 2019.

[307] Jason-Leigh Striegher, 'Violent-Extremism: An Examination of a Definitional Dilemma' [2015] The Proceedings of [the] 8th Australian Security and Intelligence Conference 75, 76.

[308] 'Education for Justice University Module Series: Radicalization & Violent Extremism' (n 306); Erroll Southers, *Homegrown Violent Extremism* (Elsevier Inc 2013) xii.

[309] Striegher (n 307); Southers (n 308) 4.

motivation behind terrorist attacks is much more complex and dependent upon numerous individual factors.[310] For instance, the Federal Bureau of Investigation (FBI) notes that 'the radicalization of an individual is a fluid process that does not have a timetable and does not always lead to action'.[311]

A number of countries have developed their own definitions of radicalisation as a part of Countering Violent Extremism policies. According to the Royal Canadian Mounted Police (RCMP), radicalisation is a process 'by which individuals − usually young people − are introduced to an overtly ideological message and belief system that encourages movement from moderate, mainstream beliefs towards extreme views'.[312] A similar definition is used by the FBI, which states that radicalisation is 'the process by which individuals come to believe their engagement in or facilitation of non-state violence to achieve social and political change is necessary and justified'.[313] In Australia, the Attorney-General's Department defines radicalisation as a process 'when a person's beliefs move from being relatively conventional to being radical, and they want a drastic change in society'.[314]

Whereas all definitions contain a similar element, setting out radicalisation as an individual transition from a moderate to an extreme mindset, there is no agreement on the relation between radicalisation and actual violence. Previous research has revealed a fundamental difference between the two corresponding categories (i.e. non-violent and

[310] Southers (n 308) xiii.
[311] Federal Bureau of Investigation Counterterrorism Division, '(U//FOUO) The Radicalization Process: From Conversion to Jihad' (Federal Bureau of Investigation Counterterrorism Division 2006) 4 <https://cryptome.org/fbi-jihad.pdf>.
[312] Royal Canadian Mounted Police, 'Radicalization - a Guide for the Perplexed' (Royal Canadian Mounted Police 2009) 1 <http://publications.gc.ca/site/eng/9.696861/publication.html> accessed 12 August 2019.
[313] Ryan Hunter and Daniel Heinke, 'Perspective: Radicalization of Islamist Terrorists in the Western World' (*FBI: Law Enforcement Bulletin*, 1 September 2011) <https://leb.fbi.gov/articles/perspective/perspective-radicalization-of-islamist-terrorists-in-the-western-world> accessed 10 August 2019.
[314] 'Preventing Violent Extremism and Radicalisation in Australia' (Attorney-General's Department 2015) <https://www.livingsafetogether.gov.au/information/Documents/preventing-violent-extremism-and-radicalisation-in-australia.PDF> accessed 10 August 2019.

violent radicalisation).[315] It should be noted that radicalisation does not always have a negative connotation,[316] nor does it lead inevitably to violence.[317] For instance, Bartlett and co-workers noted that the term 'radical' could be attributed to an individual 'who merely expresses a significant descent from prevailing [social] norms'.[318]

Striegher suggested that violent extremism is the less understood of the three terrorism-related terms.[319] The claim is exemplified by numerous contrasting definitions, which often fail to differentiate between violent extremism and terrorism.

According to the Australian Parliament, violent extremism refers to 'the beliefs and actions of people who support or use violence to achieve ideological, religious or political goals. This includes terrorism and other forms of politically motivated and communal violence'.[320]

In the view of the FBI, violent extremism encompasses 'encouraging, condoning, justifying, or supporting the commission of a violent act to achieve political, ideological, religious, social, or economic goals'.[321]

In turn, the Government of Denmark defines extremism as 'totalitarian and anti-democratic ideologies, intolerance of the views of others, hostile imagery and a division into "them" and "us"'.[322]

---

[315] Striegher (n 307) 77.
[316] See, for instance, RCMP, who stress that 'radical thinking is not necessarily problematic', Royal Canadian Mounted Police (n 312) 1.
[317] Alex S Wilner and Claire-Jehanne Dubouloz, 'Transformative Radicalization: Applying Learning Theory to Islamist Radicalization' (2011) 34 Studies in Conflict & Terrorism 418, 420.
[318] Jamie Bartlett, Jonathan Birdwell and Michael King, 'The Edge of Violence: A Radical Approach to Extremism' [2010] Demos 5, 50.
[319] Striegher (n 307) 78.
[320] Cat Barker, 'Australian Government Measures to Counter Violent Extremism: A Quick Guide' (*Parliament of Australia*) <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1415/Quick_Guides/Extremism> accessed 10 August 2019.
[321] 'What Is Violent Extremism?' (*Federal Bureau of Investigation*) <https://www.fbi.gov/cve508/teen-website/what-is-violent-extremism> accessed 10 August 2019.

Another contrasting formulation was suggested by the government of the United Kingdom, which defined violent extremism as 'vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. It [UK government] also regards calls for the death of members of our armed forces as extremist'.[323]

The UN General Assembly report on countering violent extremism found a significant difference across national practices. In several cases in particular it remains unclear whether the notion of extremism is extended to behaviour modes that are generally not covered under criminal law.[324]

Striegher stresses that the delineation of violent extremism with other terms is essential, given that all three phenomena constitute different challenges.[325] Each challenge therefore requires an individual action plan at a national level, which takes into account the context of a particular form of conduct.

4.4. Grounds for Terrorism, Extremism, and Radicalisation

Efforts to explain the reasons behind terrorist-related activities have been made in various academic areas, such as psychology, sociology and education. However, because a full discussion of terrorism roots lies beyond the scope of this study, the present section will focus on several relevant notions with respect to the regions analysed.

---

[322] Government of Denmark, 'A Common And Safe Future: An Action Plan To Prevent Extremist Views And Radicalisation Among Young People' (Government of Denmark 2009) <https://strongcitiesnetwork.org/en/wp-content/uploads/sites/5/2017/02/A-common-and-safe-future-Danish-Action-Plan-to-prevent-extremism.pdf>.
[323] Government of the United Kingdom, 'Counter-Extremism Strategy' (Government of the United Kingdom 2015) Cm 9148 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470088/51859_Cm9148_Accessible.pdf>.
[324] UN General Assembly, Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism 2016 [A/HRC/33/29] para 17.
[325] Striegher (n 307) 81–82.

The growing body of literature tends to adopt a mixed approach when explaining terrorism, extremism, and radicalisation. Within such frameworks, scholars recognise the complexity of reasons behind violent ideologies.

For instance, Sageman named three popular scientific approaches that address the motivation behind attacks carried out on behalf of al Qaeda.[326] The first category refers to micro-level analysis: that is, the search for individual reasons to commit violent acts. This approach is popular in psychology and psychoanalysis, where scholars scrutinise individual backgrounds and search for possible explanations for violent behaviour.[327] The problem is that individual case studies provide no statistical information as to how widespread and significant terrorism is; the studies cannot be generalised to the overall population. In addition, although a micro-level analysis operates on the assumption that terrorist behaviour deviates from that of the general population, it fails to provide any evidence of such 'otherness'. Moreover, by focusing on individual characteristics, microanalysis omits numerous situational factors.

The opposite approach is represented by macro-social analysis, which is devoted to sociological explanations of terrorism. The common 'root causes' include social, political, economical, historical, and cultural aspects.[328] The sociological analysis seeks to explain what kind of order provides fertile ground for terrorism. The question, however, is why – under similar conditions – do certain individuals became terrorists and others do not. The other question is what factors – cultural, historical, or political − come into play when terroristic organisations form their ideologies.

[326] Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (University of Pennsylvania Press 2008).
[327] ibid 16–20.
[328] ibid 20.

Sageman argues that − owing to the limitations of macro- and micro-level analyses − a new middle-range approach is needed, which encompasses how terrorists behave in their environment.[329] This holistic approach implicates a wide range of subjects, such as terrorists themselves, their interrelations, their social background, and stages of the recruiting process.

Hall provided a valuable notion regarding terrorist motivation, addressing both the perpetrator's and the victim's ideologies – political, religious, and so forth – as an explanation for attacks.[330] In the view of Krieger and Meierrieks, there are seven motives for terrorist activities:[331]

- economic deprivation (social inequality and poverty);
- socio-economic and demographic strain (modernisation may cause a transformation in the labour market and discontent among citizens who have lost their jobs);
- political and institutional order (in particular states);
- political transformation and instability;
- identity and cultural clash (different ethnic and religious groups may cause conflicts within the country);
- global economic and political order (globalisation);
- contagion (countries affected by terrorism are likely to suffer from new terrorism movements, and terrorism may spread to neighbouring countries).

[329] ibid 23–25.
[330] Harold Hall (ed), *Terrorism: Strategies for Intervention* (The Haworth Press 2003) 2.
[331] Tim Krieger and Daniel Meierrieks, 'What Causes Terrorism?' (2011) 147 Public Choice 3.

Wilner and Dubouloz[332] name three following precursors of homegrown terrorism[333] and radicalisation: socio-political alienation, religiosity and globalisation, and reaction to foreign policy. Socio-political alienation means that citizens who are poorly integrated within a host or native country will search for alternative groups with which to associate. In turn, aggressive religious groups − e.g. jihadists − have a sensitive perception of changes brought about by globalisation and the erosion of cultural identity. The third reason could be attributed to disagreement with the foreign policy of a host or native country, especially when it comes to engaging in military conflicts.

The UN General Assembly report relied on 'push' and 'pull' factors when addressing extremism.[334] Whereas 'push' factors that drive extremism are external impacts and context, 'pull' factors are individual motivations leading to violent actions. In particular, the report addresses the five following 'push' conditions behind extremism: 1) lack of socioeconomic opportunities; 2) marginalisation and discrimination; 3) poor governance, violations of human rights and rule of law; 4) prolonged and unresolved conflicts; and 5) radicalisation. In turn, 'pull factors' include individual background and motivation; collective grievances and victimisation – when one nation has historically suffered under other nation; the misuse of beliefs – whether political, religious, or referring to ethnic difference; and the existence of charismatic leaders and informal social networks defending radical views.

Although economic inequality, globalisation, and individual backgrounds appear to be common factors in the above frameworks, the author believes that ethnic factors play a pivotal role in driving extremism views across the post-Soviet countries. This assumption is based on the infamous history of forced deportations in the Soviet Union, which affected

[332] Alex S Wilner and Claire-Jehanne Dubouloz, 'Homegrown Terrorism and Transformative Learning: An Interdisciplinary Approach to Understanding Radicalization' (2010) 22 Global Change, Peace & Security 33.
[333] The opposite of international terrorism is when terrorists attack civilians in their native country. See Southers (n 308) 6.
[334] UN General Assembly, Plan of Action to Prevent Violent Extremism 2015 [A/70/674] paras 24–37.

approximately 60 nationalities and millions of lives from the1920s to the 1950s.[335] The ethnic groups in North Caucasus, in Crimea and other parts of Ukraine, in Moldova and Poland, and in the Baltic States were among those that were relocated during that period. As a result of these large-scale population transfers, numerous internal diasporas were formed across the Soviet Union. In the period of the USSR's dissolution and the rise of national sentiments in the former republics, the territories affected by deportations became a bone of contention in state policies. Polian gives a figure of 300 territorial claims that were put on the table between 1988 and 1996, nearly 140 of which remained unresolved as of the 2000s, and six of which sparked regional wars.[336]

Considering these tensions, the spreading of radical and extremist views in the countries analysed is largely driven by ethnic composition. As the author stresses in this section, research in the field of political science supports the hypothesis that countries with ethnic minority groups geographically concentrated in one part of the country, and ethnic groups with kin in other countries, are more likely to experience terrorism.[337] Such minority groups could be exposed to separatist sentiments, while compatriots from abroad may provide financial and political support. For diasporas, terrorist attacks could become a form of achieving their goals with respect to majority populations.

The long history of deprivation imposed by hosting countries on diasporas might aggravate the situation.[338] In such conditions, the grievances become a basis for minorities to establish a social movement, and to 'fuel' terrorism as an extreme form of resolving frustration – either by achieving social equality or by forming an independent state.

---

[335] Nikolaĭ Bugaĭ, *The Deportation of Peoples in the Soviet Union* (Nova Publishers 1996) 2.
[336] Pavel Polian, *Against Their Will: The History and Geography of Forced Migrations in the USSR* (Central European University Press 2003) 226.
[337] *See* Bryan J Arva and James A Piazza, 'Spatial Distribution of Minority Communities and Terrorism: Domestic Concentration versus Transnational Dispersion' [2016] Defence and Peace Economics 3.
[338] Martha Crenshaw, 'The Causes of Terrorism' (1981) 13 Comparative politics 379, 383.

By way of illustration, because of the history and ethnic composition of the North Caucasus region,[339] Russia joins the United Kingdom,[340] the Netherlands,[341] Turkey,[342] France, and Spain[343] in the long list of European states in which political violence and terrorism have a religious and an ethnic basis, and where the authorities are constantly seeking ways to mitigate the threat of a terrorist attack.

4.5. Approaches to National Security in the Post-Soviet Countries

The disintegration of the USSR brought significant changes to security-related order on the Eurasian continent. One change that had considerable impact was the establishment of a new logic of military cooperation with multiple sub-regional groups and of new military alliances. Whereas the Eastern European states from the Visegrád Four[344] and the Baltic states were integrated into the NATO alliance, the other countries from the former Soviet Union were at a crossroads when deciding on a new security agenda.[345] New leading and medium powers entered into the competition for the region, such as Russia, the EU, the United States, China, Iran, and Turkey.[346] Since the collapse of the Soviet Union, post-Soviet countries have faced new security challenges, most notably related to frozen conflicts and to establishing criminal fiefdoms in these problematic territories, and to the proliferation of military technology and small arms.[347]

---

[339] *See, in general,* Monica Duffy Toft and Yuri M Zhukov, 'Denial and Punishment in the North Caucasus: Evaluating the Effectiveness of Coercive Counter-Insurgency' (2012) 49 Journal of Peace Research 785.
[340] *See* Richard English, *Armed Struggle* (Pan 2005) 3–4.
[341] *See* Maria M Komen, 'Homegrown Muslim Extremism in the Netherlands: An Exploratory Note' (2014) 7 Journal of Strategic Security 47.
[342] *See* Yonah Alexander, Edgar H Brenner and Serhat Tutuncuoglu Krause, *Turkey: Terrorism, Civil Rights, and the European Union* (Routledge 2008).
[343] *See* Teresa Whitfield, 'The Basque Conflict and ETA' (United States Institute of Peace 2015) <https://www.usip.org/sites/default/files/SR384-The-Basque-Conflict-and-ETA-The-Difficulties-of-An-Ending.pdf> accessed 13 August 2019.
[344] Czech Republic, Hungary, Poland and Slovakia
[345] Andrew Cottey, 'The Other Europe: Regional Security Governance in Europe's East' in Shaun Breslin and Stuart Croft (eds), *Comparative regional security governance* (Routledge 2012).
[346] ibid 47.
[347] ibid 47–50.

The Soviet legacy posed some rationale for remaining a distinctive geopolitical space. This idea became dominant in Russia, which tried to reintegrate former Soviet republics under its lead. As noted by Rumer, no geopolitical objective of the Russian Federation 'has been articulated more frequently, clearly, or with greater consistency throughout the post-Soviet period than the consolidation of a Russian sphere of influence among the former countries of the Soviet Union'.[348]

However, because Russia would remain a leading power, some republics have opposed this approach, and are in search of an alternative direction. This tension may be observed, for instance, in the politics of the GUAM states (Georgia, Ukraine, Azerbaijan, Moldova).[349] Along these lines, the development of regional security policies was framed basically, on the one hand, by Russian attempts to rebuild a distinctive security space within former Soviet republics, and, on the other hand, by the resistance to this ambition by some of the other FSU republics.[350]

Multilateral and bilateral agreements may serve as a useful basis when analysing the logic of the regional security agenda within the post-Soviet region, the interconnections, and the objectives of the states. The major sub-regional security groups are represented by the Commonwealth of Independent States (CIS), the Collective Security Treaty Organisation (CSTO), the Organisation for Democracy and Economic Development (GUAM), and the Shanghai Cooperation Organisation (SCO).

The Commonwealth of Independent States (CIS) is an intergovernmental organisation formed by the successor countries of the former USSR, and was established by a set of agreements during the period 1991-1993.[351] The organisation currently includes ten former

[348] Eugene B Rumer, *Russian Foreign Policy beyond Putin* (Routledge 2017).
[349] Cottey (n 345) 45.
[350] ibid 51.
[351] ibid.

Soviet republics. Apart from economical, law-making, and diplomatic cooperation, the parties collaborate on military affairs.

At the outset, the CIS should have developed an approach involving long-term military collaboration within the FSU, although the parties – with the exception of Russia – virtually show limited participation involving security matters.[352] The set of military-related activities within the CIS is represented, *inter alia*, by peacekeeping operations. The latter includes four missions: namely, in Transnistria (from 1992), Tajikistan (from 1993 until 1999), South Ossetia (from 1992 until 2008), and Abkhazia (from 1992 until 2008).[353] Nonetheless, these nominally CIS operations were Russian for the most part, pursuing Russian-oriented goals under the guise of having comprehensive support from other CIS republics.

Owing to this minimal efficiency, integration efforts in the area of security since the 2000s have fallen within the scope of the Collective Security Treaty Organisation.[354] A Collective Security Treaty establishes an agreement on collective defence between signatories, akin to Article 5 of the North Atlantic Treaty. Despite the fact that the organisation's effectiveness is commonly doubted by experts, and contested by other regional organisations such as the SCO, it remains an important part of the Russian security agenda.[355]

The Organization for Democracy and Economic Development (GUAM) is yet another regional organisation in post-Soviet space. By and large, the institution was built on the mutual desire of the member states to contest Russian dominance in the area.[356] GUAM was established in October 1997 at the Council of Europe Summit. Among the range of activities,

---

[352] ibid.

[353] See, in general, Dov Lynch, *Russian Peacekeeping Strategies in the CIS: The Case of Moldova, Georgia and Tajikistan* (Springer 1999); Alexander Sokolov, 'Russian Peace-Keeping Forces in the Post-Soviet Area' (1997); Cottey (n 345) 51.

[354] See Section 3.3, *'Interconnectedness of the post-Soviet region: means and narratives'*.

[355] Tsygankov (n 46) 421.

[356] Cottey (n 345) 54.

the organisational goals imply the promotion of democratic values, the bolstering of international and regional security, and the enhancing of European integration. The GUAM Charter contains a clause regarding 'common security space'.[357] In general, cooperation within GUAM is weak, with the parties having to coordinate their activities in various multilateral frameworks such as the CIS and the OSCE.

The Shanghai Cooperation Organisation (SCO)[358] was established in June 2001 by the leaders of China, Russia, Kyrgyzstan, Kazakhstan, Uzbekistan, and Tajikistan. In 2017, the SCO was joined by two new member states represented by India and Pakistan. The pivotal distinction of the institution rests with the membership of a powerful non-FSU actor such as China.[359] Therefore, Russia cannot take exclusive leadership in the SCO, and the efficiency of the organisation revolves around relations between China and Russia. In addition, the SCO represents a regular cooperative security organisation with respect to the aim of lowering the danger of warfare and conflicts between the parties (mainly China and Russia).[360] As to the organisational goals, the Shanghai Convention addresses 'terrorism, separatism, and extremism' as major threats requiring countermeasures.[361] It should be noted that even though the heads of member states do not position the SCO as being an institution in opposition to NATO or the US, during meetings the leaders emphasise the need to oppose Western dominance in the international arena.[362] In recent years, SCO states have increased

[357] GUAM, 'Charter of Organization for Democracy and Economic Development' (*GUAM*, 22 April 2006) <http://guam-organization.org/en/charter-of-organization-for-democracy-and-economic-development-guam/> accessed 16 August 2019.
[358] See, in general, Tsygankov (n 46) 400–408.
[359] Alyson JK Bailes, Vladimir Baranovsky and Pál Dunay, 'Regional Security Cooperation in the Former Soviet Area' (2007) 2007 SIPRI Yearbook 174, 184.
[360] Cottey (n 345) 56.
[361] Shanghai Cooperation Organization (SCO), 'Shanghai Convention on Combating Terrorism Separatism and Extremism' (15 June 2001) <https://www.un-ilibrary.org/peacekeeping-and-security/international-instruments-related-to-the-prevention-and-suppression-of-international-terrorism_d6956b09-en> accessed 16 August 2019.
[362] Cottey (n 345) 56.

cooperation in the area of security, which has taken the forms of joint training and counter-terrorism operations.[363]

The cooperation through regional organisations as well as multilateral and bilateral agreements has had a particular impact in developing common strategies regarding national security throughout the post-Soviet region. Such practices have been extended to information security matters.[364] Information security in the region has been established, *inter alia*, owing to the need to counter cyber-attacks and data breaches, but also on the basis of the regimes' fear of popular social protest.[365] The approach towards the Internet by regional authorities can be explained partially in terms of a general wariness regarding the free flow of information as well as the historical tradition of censoring any kind of media. In turn, regional normative frameworks affect the global agenda on online regulation as well as the perception of linkages between the Internet and national security.

In recent years, a number of analysed countries have introduced doctrines on 'information security', using wording similar to that of the Russian Information Security Doctrine of 2000 and 2016.[366] The current Doctrine of 2016 announces 'the sovereignty of the Russian Federation in the information sphere' as a national security interest.[367] Paragraph No. 12 notes, *inter alia*, that foreign media publish 'biased' information about Russian national policy, and there is 'increased information-related impact on the Russian population, especially the youth, aimed at erasing traditional […] spiritual values'. In a similar manner, the Belarusian Concept of National Security from 2001 introduced a section on the risks of

[363] Bailes, Baranovsky and Dunay (n 359) 186–187.
[364] Jaclyn A Kerr, 'Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region' (2018) 12 International Journal of Communication 3814, 3823.
[365] ibid.
[366] ibid.
[367] The Decree of the President of the Russian Federation 'On Informational Security Doctrine of the Russian Federation' 2016 [646] para 8.d.

the Internet to information security.[368] The current Concept of National Security was introduced in 2010, recognising that information technologies may facilitate 'the practice of targeted information pressure […], which causes significant harm to national interests'.[369] On 18 March 2019, the Belarus Security Council adopted a Concept of Informational Security. The Concept contains a clause regarding 'destructive information influence': that is, 'an informational influence on political and socio-economic processes, operation of public authorities, […] in order to weaken a state defence capacity, adopting knowingly disadvantageous decisions'.[370] Since 2002, the Law of Uzbekistan on Principles and Guarantees on Access to Information has stipulated protection against information 'calling for violent change of constitutional order, undermining the territorial integrity and sovereignty of Uzbekistan, seizure of power from elected and appointed authorities, or any infringement against institutional order'.[371] Kazakhstan's 2002 Law on National Security announced, *inter alia*, threats 'reducing manageability in the country' and 'informational impact on public and individual opinion, [..] dissemination of false information harming national security'.[372]

In Kyrgyzstan, the Concept for Information Security of 2005 was among the first efforts to describe national interests in the sphere of information. The document was criticised for its vague definitions of 'state secrets', 'commercial secrets', and 'private information', which could lead to broad interpretation and abuse.[373] On 3 May 2019, the

[368] Miklos Haraszti and others, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Mit Press 2010) 166.
[369] Decree of the President of the Republic of Belarus 'On approval of the National Security Concept of the Republic of Belarus' 2010 [575].
[370] Resolution of the Security Council of the Republic of Belarus 'On the Concept of Informational Security of the Republic of Belarus' 2019 [1].
[371] The Law of the Republic of Uzbekistan 'On Principles and Guarantees on Access to Information' 2002 [439–II] Art. 15.
[372] The Law of the Republic of Kazakhstan 'On the National Security of the Republic of Kazakhstan' 2012 [527–IV] Art. 6.
[373] Haraszti and others (n 368) 196.

Kyrgyz government approved the Information Security Concept for 2019-2023, which repeated state security concerns similar to those established in Russia and Belarus. For instance, paragraph 15 recognises that 'global mass media' play an important role in the political, economic, and social agenda, and fundamental changes recently taking place around the globe have been achieved through 'new technologies of mass control'.[374] In the subsequent paragraph, the government notes that widespread use of the Internet by the Kyrgyz population 'paves the way for targeted impact on the domestic political situation to the detriment of national interests'.

As already mentioned in this section, regional organisations play an important role in spreading similar regulatory frameworks. For instance, in September 2012, leaders of the CIS countries expressed an idea about establishing a CIS Cyber-security Centre akin to the framework of the Community Emergency Response Team (CERT).[375] Prior to this event, the research centre of the Russian Communication Ministry held training courses for information security experts from CIS countries.[376]

Within the CSTO, there were efforts in 2011 to create a single system to control harmful online sources, probably as a response to the 'destructive' impact of social networks during the Arab Spring events.[377]

According to Nikolay Bordyuzha, then General Secretary of the CSTO, in December 2010 the organisation detected 2000 objectionable webpages that could bring 'political

---

[374] 'Pravitel'stvo utverdilo Kontseptsiyu informatsionnoy bezopasnosti Kyrgyzstana na 2019-2023 gody [The Government approved the Information Security Concept of Kyrgyzstan for 2019-2023]' (*Today.KG*, 17 May 2019) <https://today.kg/news/59446/> accessed 18 August 2019; Resolution of the Government of the Republic of Kyrgyzstan 'On Information Security Concept of Kyrgyzstan for 2019-2023' 2019 [209].

[375] Andrei Soldatov and Irina Borogan, 'In Ex-Soviet States, Russian Spy Tech Still Watches You' [2012] *Wired* <https://www.wired.com/2012/12/russias-hand/> accessed 18 August 2019.

[376] ibid.

[377] Joshua Kucera, 'With Eye To Arab Spring, CSTO Strengthens Cyber, Military Powers' (*Eurasianet*, 15 August 2011) <https://eurasianet.org/with-eye-to-arab-spring-csto-strengthens-cyber-military-powers> accessed 18 August 2019; Kerr (n 364) 3825.

damage' to CSTO countries.[378] Borduyzha expressed concern that former Soviet republics were being 'manipulated' through online content disseminated by certain political forces referring to movements such as the Colour Revolutions. Therefore, information security has a broad scope of application in the CSTO agenda, not only with respect to data protection and cyber-attacks but also to securing political regimes.

A similar approach is promoted through SCO cooperation.[379] SCO leaders often advocate the need to strengthen the e-sovereignty of the states and the right of authorities to establish Internet policies.[380]

At the same time, an institution encouraged governments to cooperate jointly in countering terrorism and extremism information. There were efforts to promote regional frameworks at the international level, such as an 'International Code of Conduct for Information Security' from September 2011, suggested by China, Russia, Uzbekistan, and Tajikistan at the UN General Assembly session.[381] However, the proposition was interpreted ambiguously, and did not find international support.[382] The proposal was suggested again in January 2015. Some experts argued that the initiative was simply a Russian-Chinese effort to

[378] Joshua Kucera, 'CSTO Fires Salvo in Information War' (*Eurasianet*, 27 December 2010) <https://eurasianet.org/csto-fires-salvo-in-information-war> accessed 18 August 2019; Kerr (n 364) 3825.
[379] Kerr (n 364) 3826.
[380] For instance, in June 2011, at the CSO summit in Astana, Kazakhstani President Nursultan Nazarbayev stressed that 'it was a time to include the concept of 'electronic borders' and 'e-sovereignty' in international law. See Andrei Soldatov and Iryna Borodan, 'Russia's Surveillance State' (12 September 2013) <https://worldpolicy.org/2013/09/12/russias-surveillance-state/> accessed 5 July 2019.
[381] Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, Letter to the United Nations addressed to the Secretary-General: Developments in the field of information and telecommunications in the context of international security 2011 [UN A/66/359].
[382] Jeffrey Carr, '4 Problems with China and Russia's International Code of Conduct for Information Security' (*4 Problems with China and Russia's International Code of Conduct for Information Security*, 22 September 2011) <http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html> accessed 18 August 2019; Nate Anderson, 'Russia, China, Tajikistan Propose UN "Code of Conduct" for the 'Net' (*Ars Technica*, 20 September 2011) <https://arstechnica.com/tech-policy/news/2011/09/russia-china-tajikistan-propose-un-code-of-conduct-for-the-net.ars> accessed 18 August 2019; Kerr (n 364) 3827.

justify harsh Internet regulations at the international level in order to prevent social protests in their own countries.[383]

4.6. Freedom of Expression: General Approaches and Limitations to National Security

Freedom of opinion and expression is a universally recognised human right, established in all international human rights doctrines as well at the state level.[384] In the Universal Declaration of Human Rights (UDHR), the right is protected under Article 19, reading as follows:

> *Everyone 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*.[385]

A similar wording is suggested in Article 19 of the International Covenant on Civil and Political Rights (ICCPR), although the later document formulates the scope of the right in a more precise manner. In particular, the ICCPR stipulates that freedom of expression extends to information and ideas 'of any kind […] either orally, in writing or in print, in the form of art, or through any other media of his choice'.[386] Such a formulation provides a useful hint as to what 'expression' means in customary law. Further clarification can be gleaned from the UN's general comment, which stresses that all kinds of information are to be protected, including 'political discourse, commentary on one's own and on public affairs,

[383] Kerr (n 364) 3827.
[384] See, in general, Emily Howie, 'Protecting the Human Right to Freedom of Expression in International Law' (2018) 20 International journal of speech-language pathology 12.
[385] UN General Assembly, Universal Declaration of Human Rights 1948 [217 A (III)].
[386] UN General Assembly, International Covenant on Civil and Political Rights 1966 [999 UNTS 171].

canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching and religious discourse'.[387]

Drawing from legal traditions of 'old democracies', it seems that two distinctive discourses were established in the European Union and in the United States with regard to freedom of expression. In the US, the respective right has its roots in the First Amendment, adopted as early as 1791, which rules that:

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*.[388]

In the EU, the right to freedom of expression is enshrined in Article 10 of the European Convention on Human Rights (ECHR), which states that:

> *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers*.[389]

At the outset, one may note the difference in formulating the right: namely, 'freedom of speech' vs. 'freedom of expression'. From the linguistic point of view, these terms have an uneven scope: 'speech' is about verbal communicating and the formulation of ideas, whereas 'expression' is any act of representing the information.[390] Moreover, Sidak points out the

---

[387] UN Human Rights Committee, General comment No. 34. Article 19: Freedoms of opinion and expression 2011 [CCPR/C/GC/34] para 11.
[388] U.S. Const. amend. I
[389] European Convention on Human Rights (n 275).
[390] Cf 'expression' and 'speech' at 'Dictionary by Merriam-Webster' <https://www.merriam-webster.com/> accessed 14 August 2019.

difference between precise speech and 'ambiguous' expression.[391] In practice, however, the terms are used interchangeably in the US and the EU, covering a wide variety of expression formats, whether academic articles, artistic works, national or ethnic attributes, or any kind of symbolic expression.[392]

In both frameworks, freedom of expression is not an absolute right, but can be limited under numerous conditions. In the US, such categories include fighting words, obscenity, advocacy of illegal action, and commercial speech.[393] Article 10 of the ECHR implies limitations protecting health or morals, reputation, and security-related matters, which the author describes in the following section. The inciting of ethnic and religious hatred and denying the Holocaust are also restrictions widely present in national frameworks.[394] Nevertheless, the major difference between the US and the EU approach lies in the limitation of admissible intolerant statements.[395]

The US judiciary is generally 'overprotective' of freedom of speech, even when it comes to sensitive topics and to hate speech. For instance, in the prominent case of *Brandenburg v Ohio*, the Court found no violations in the rally speech of Clarence Brandenberg, a Ku Klux Klan leader in rural Ohio.[396] The Court set up a clear requirement that the speech was not to be prohibited unless it led 'to imminent lawless action'. Furthermore, viewing the case *National Socialist Party of America v Village of Skokie*, the Supreme Court protected an opportunity of the neo-Nazi party to immediately appeal a lower

[391] J Gregory Sidak, 'Some Economics of Flag Burning and Jimi Hendrix' (2016) 1 Criterion J. on Innovation 563.
[392] See, for instance, Wolfgang Benedek and Matthias C Kettemann, *Freedom of Expression and the Internet* (Council of Europe 2013) ch 2.
[393] 'First Amendment' (*Legal Information Institute*, 6 August 2007) <https://www.law.cornell.edu/wex/first_amendment> accessed 14 August 2019.
[394] Benedek and Kettemann (n 392) 46, 81.
[395] Robert A Sedler, 'An Essay on Freedom of Speech: The United States versus the Rest of the World' [2006] Mich. St. L. Rev. 377; Mila Versteeg, 'What Europe Can Teach America About Free Speech' (*The Atlantic*, 19 August 2017) <https://www.theatlantic.com/politics/archive/2017/08/what-europe-can-teach-america-about-free-speech/537186/> accessed 14 August 2019.
[396] *Brandenburg v Ohio* [1969] US Supreme Court 395 U.S. 444.

court's decision that would have restricted their march in the predominantly Jewish village of Skokie. This Supreme Court decision opened a door for the NSPA to hold their events.[397] Such an unprecedented level of tolerance involving hate speech is argued by some scholars to be culturally specific to the US.

In European states, owing to the terrible legacy of the Second World War, any expression sympathising with the Nazi regime is strictly prohibited. At the same time, it should be noted that within the EU approach the right to freedom of expression implies the right to shock and offend. The European Court of Human Rights ruled in *Handyside v United Kingdom* that Article 10 is applicable 'not only to 'information' or 'ideas' that are favourably received […], but also to those that offend, shock or disturb the State or any sector of the population'.[398]

Protecting the right to freedom of opinion and expression has both individual and social significance. In the view of the UN Human Rights Committee, freedom of expression is crucial for personal development as well as for the establishment of a democratic society.[399] Freedom of expression is essential in upholding associated fundamental rights, including the right of assembly and association, and the right to education.[400] In recent years, however, there has been an increasing number of cases involving unreasonable limitations of expression, even in democratic societies.[401] Such measures are commonly justified by reasons relating to national security.

As mentioned above, the protection of freedom of expression offered by international and national legal instruments is not absolute, since this right often has to be reconciled with

---

[397] *National Socialist Party of America v Village of Skokie* [1977] U S Supreme Court 432 US 43.
[398] *Handyside v United Kingdom* [1976] ECtHR 5493/72.
[399] UN Human Rights Committee General comment No. 34. Article 19: Freedoms of opinion and expression (n 387) para 2.
[400] Benedek and Kettemann (n 392) 39.
[401] Howie (n 384).

conflicting policy objectives such as the fight against illegal or harmful content. For instance, the European Convention of Human Rights stipulates that this right

> *may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*[402]

Similar limitations can be found in other international treaties and national legal instruments,[403] and the interpretation of such provisions can have a profound impact on both the public and the private sector.[404] However, the self-directing or unguided reading of such restrictions may lead to a disproportional and unnecessary curbing of freedom of expression. Individuals seeking to exercise this right can encounter all kinds of government-imposed limitations (introduced with goals such as combatting defamation or hate speech online), which result in an unfortunate situation when − in the words of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression − 'targets of restrictions include journalists and bloggers, critics of government, dissenters from

[402] Article 10, European Convention on Human Rights. It should be noted that Article 10 of the Convention also applies to the various forms and means by which it is transmitted and received, since any restriction imposed on the means necessarily interferes with the right to receive and impart information (See, 'Internet: Case-Law of the European Court of Human Rights' (Council of Europe 2015) 40 <https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> accessed 14 June 2019.).

[403] Adrienne Stone, 'The Comparative Constitutional Law of Freedom of Expression' in Tom Ginsburg and Rosalind Dixon (eds), *The Comparative Constitutional Law* (Edward Elgar 2011).

[404] For instance, intermediary liability for third-party behaviour is a concept introduced recently into the discussion concerning freedom of expression on the Internet; see, *Delfi AS v Estonia* [2015] Grand Chamber ECtHR 64569/09.

conventional line, provocateurs and minorities of all sorts'.[405] In this regard, courts act as the last line of defence, deciding or defining whether the laws or administrative practices that, on the surface, have a legitimate purpose, are not 'a pretext for blocking or censoring the Internet'.[406] Moreover, issues such as public morality or national security are notoriously difficult to define precisely. In this domain, a case-by-case examination by competent courts may be the only way forward to distinguish between what does and what does not fall under the freedom of expression protections.[407]

4.7. Freedom of Expression Online: the Internet as a New Paradigm-Shifting Media

The recent estimates on Internet usage report a daily audience of 4.4 billion people worldwide, or 57 percent of the global population.[408] Over the last decade, the Internet has become a vital communication and information medium, which makes it an important regulatory area where human rights must be ensured, including the right to freedom of expression.

From the outset, human rights protection on the Internet has been rooted in the general principle that 'what applies offline, applies online'.[409] Nonetheless, the specific nature of the Internet makes its adjustment to national legal frameworks and judicial decisions necessary, particularly in the practice of the European Court of Human Rights. By way of illustration, in the case *Editorial Board of Pravoye Delo and Shtekel v Ukraine*, the

---

[405] Kaye D, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 2016 [A/71/373] para 55.
[406] Patrick Ford, 'Freedom of Expression through Technological Networks: Accessing the Internet as a Fundamental Human Right' (2014) 32 Wis. Int'l LJ 142, 170.
[407] For instance, see, *Perrin v UK* [2005] ECtHR 5446/03.
[408] Simon Kemp, 'Digital 2019: Global Internet Use Accelerates' (*We Are Social*, 30 January 2019) <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates> accessed 18 July 2019.
[409] Resolution of the Human Rights Council 'On The promotion, protection and enjoyment of human rights on the Internet' 2012 [A/HRC/20/8].

court stressed the difference between the Internet and analogue media in terms of the ability to store and transmit information:

> *The electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned*.[410]

When referring to the 'specific nature' of the Internet, numerous attributes should be taken into account. In 2016, the European Court of Human Rights Judge, Robert Spano, acknowledged that the Internet in its current state is unique, as a rich variety of content is made immediately available to anyone who can afford the relatively minimal cost of access; individuals can communicate their views, ideas, and thoughts to others; and individuals have equal opportunities for communication.[411]

The recent trend in Internet development is a 'shift towards mass participation in content creation', extending participation and fostering novel means with regard to the exchange of knowledge.[412] People may prefer using the World Wide Web to prior forms of media (such as television networks) and communication (such as telephone), because the

---

[410] *Editorial Board of Pravoye Delo and Shtekel v Ukraine* [2011] ECtHR 33014/05 [63].
[411] Robert Spano, *The Internet and the ECHR - A Paradigm Shift?* (2016) <http://tv.coe.int/ECHR/video.php?v=ECHR_20160118_Spano> accessed 5 February 2018.
[412] Daniel Kilburn and Jonathan Earley, 'Disqus Website-Based Commenting as an e-Research Method: Engaging Doctoral and Early-Career Academic Learners in Educational Research' (2015) 38 International Journal of Research & Method in Education 288.

Internet allows 'multiway' simultaneous forms of communication, and gives users the ability to reach large numbers of people very quickly.[413]

The media's switch from offline to the digital world has happened simultaneously with the expansion of the scale on which modern journalism operates. Back in pre-Internet times, the proliferation of media was limited by the constraints of the physical world: 'the airwaves could handle only so many TV and radio programs, shops could stock only so many books and records, and movie theatres could screen only so many films'.[414] These constraints (high costs and narrow distribution channels) are currently disappearing, as 'the virtual shelves of the Internet can expand to accommodate everything'.[415] In short, anybody who has Internet access is now a journalist.[416] This situation has profound implications when it comes to media-related freedom,[417] as it has long been acknowledged that the media perform an essential function in a democratic society, and play a vital role in the form of public watchdog[418] and purveyor of information.[419]

At the same time, there is an elevated risk of 'fake news' being spread by either uneducated or ill-intentioned individuals. Under this 'umbrella term', the author refers to information that has been deliberately twisted or fabricated, and disseminated with the intention of deceiving and misleading others into believing falsehoods or doubting verifiable

---

[413] Ford (n 406) 144–145.
[414] Nicholas Carr, *The Big Switch: Rewiring the World, from Edison to Google* (WW Norton & Company 2008) 149.
[415] ibid 150.
[416] Rephrased statement of Sandra Mims Rowe, an editor for the Portland Oregonian in 1999, cited from Knowledge Mushohwe, 'Everyone Is Now a Journalist, Thanks to the Internet' (*The Herald*) <https://www.herald.co.zw/everyone-is-now-a-journalist-thanks-to-the-internet/> accessed 6 July 2018.
[417] Move of media online and the challenges of balancing freedom of expression with other human rights are further corroborated in several high-profile cases before international courts, such as *Delfi AS v Estonia*, cited above.
[418] *The Sunday Times v The United Kingdom* [1979] ECtHR 6538/74.
[419] *Barthold v Germany* [1985] ECtHR 8734/79.

facts.[420] All of the above means that when it comes to the Internet as a form of media, the balancing of various human rights is an extremely precarious exercise, since all-encompassing and universal rules are either almost or entirely impossible to define.[421] The authorities (including the courts) should be careful in limiting forms of online expression while combatting fake news: namely, 'an entire village should not be burned to roast a pig'.[422]

Additionally, whereas the pre-Internet regulatory frameworks were developed under the premise that all legal actions are geographically limited, this is not the case in the online world.[423] The actions are taking place simultaneously, under multiple jurisdictions. In the 2011 Report, Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, referred to 'speed, worldwide reach and relative anonymity' as being unique features and advantages of the Internet.[424] Such characteristics became a powerful democratic tool, as citizens were granted the power to disseminate information to a large audience in 'real time', and to mobilise and coordinate protests.

One of the most notable and the first example of 'digital activism' was represented by the Arab Spring uprisings – a wave of revolutions that took place in North Africa and the Middle East in the 2010s. Starting with the Tunisian revolution, anti-government protests spread rapidly to other countries in the region, such as Egypt, Libya, and Syria. About the

---

[420] See Tarlach McGonagle, '"Fake News" False Fears or Real Concerns?' (2017) 35 Netherlands Quarterly of Human Rights 203.

[421] In Europe, for instance, false stories and conspiracy theories presented as news and that constitute racist expression, incitement to hatred, or denial of the Holocaust will not benefit from freedom of expression protection. Satire, however, does enjoy protection, as it is a form of artistic expression and social commentary, and, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate. See *Supra* McGonagle.

[422] *Supra* McGonagle.

[423] Oreste Pollicino and Marco Bassini, 'The Law of the Internet between Globalisation and Localisation' [2014] Transnational Law: Rethinking European Law and Legal Thinking, Cambridge UP 346, 348–349.

[424] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 2011 [A/HRC/17/27] para 23.

same time, protest movements occurred throughout democratic regimes as well.[425] Although the extent to which digital platforms 'sparked' these uprisings is debated,[426] there is general agreement that Internet technologies became a visible factor. One of the prominent activists behind the uprisings in Egypt, Wael Ghonim, named the protest 'Revolution 2.0', and commented, 'I want to meet Mark Zuckerberg one day and thank him...if you want to liberate a society just give them the Internet'.[427]

At the same time, the regions under scrutiny faced their own waves of popular protests in recent years – for instance, the colour revolutions of the mid-2000s, the Euromaidan of 2014 in Ukraine, and so on. In the Orange Revolution in Ukraine,[428] experts were already commenting on the role of electronic communication in social mobilisation; however, this role was less evident in comparison to the Arab Spring events.

In popular protests, digital platforms served not only as communication tools but they also contested the existing power-relations in forming the views of the population. Whereas public opinion in the pre-Internet era was formed by 'newsroom elites', digital platforms challenged the dominance of traditional media as 'information gatekeepers'. [429] This development was crucial, especially in the sense that analogue media could be controlled and financed by the state regime.

At the same time, Internet technologies presented new challenges regarding fundamental human rights, with the major challenges represented by global surveillance,

---

[425] Simon Lindgren, *Digital Media and Society* (Sage 2017) 220.

[426] Simon Cottle, 'Media and the Arab Uprisings of 2011' (2011) 12 Journalism 647; Merlyna Lim, 'Clicks, Cabs, and Coffee Houses: Social Media and Oppositional Movements in Egypt, 2004–2011' (2012) 62 Journal of communication 231; Mathew Ingram, 'Was What Happened in Tunisia a Twitter Revolution?' (*Gigaom*, 14 January 2011) <https://gigaom.com/2011/01/14/was-what-happened-in-tunisia-a-twitter-revolution/> accessed 20 August 2019; Malcolm Gladwell, 'Does Egypt Need Twitter?' <https://www.newyorker.com/news/news-desk/does-egypt-need-twitter> accessed 20 August 2019.

[427] Lim (n 426) 232.

[428] Myroslaw J Kyj, 'Internet Use in Ukraine's Orange Revolution' (2006) 49 Business Horizons 71.

[429] Sharon Meraz and Zizi Papacharissi, 'Networked Gatekeeping and Networked Framing On# Egypt' (2013) 18 The international journal of press/politics 138.

personal data gathering, and data protection.[430] The demands of a democratic society and its obligations towards protecting individual rights must be balanced against the need and desire for electronic commerce and information technology. The right to a private life – that is, the right not to be 'subjected to arbitrary interference with his privacy, family, home or correspondence' as per Article 12 of the Universal Declaration of Human Rights – is also one of the universally applicable human rights.[431] Nevertheless, the post-9/11 era 'can be characterised by the desire and ability of governments to develop a global mass surveillance system, largely unseen and until recently unsuspected', and 'a common trend can be discerned whereby governments monitor the communications and online behaviour of the vast majority of ordinary citizens'.[432] Recent times have witnessed an 'increase in international police and judicial activities to fight terrorism and other forms of international organised crime, supported by an enormous exchange of information for law enforcement purposes'.[433]

Private companies jumped gleefully onto a surveillance and data-gathering bandwagon, collecting information on online users that could later be used for marketing purposes,[434] or even for more nefarious reasons, as the recent Cambridge Analytica scandal demonstrated.[435] In this sphere, court adjudication proved to be an effective way of keeping

---

[430] See, for general discussion, Eady D. (2015) Privacy: A Judicial Perspective. In: J. Lewis et al., eds., *Media Law and Ethics in the 21st Century*. New York: Macmillan, pp. 3-34.

[431] Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) 2 Groningen Journal of International Law 33, 37–42. This right is enshrined in Article 17 of the International Covenant on Civil and Political Rights, Article 16 of the United Nations Convention on the rights of the child, Article 8 of the European Convention on Human Rights and so on.

[432] Arianna Vedaschi and Valerio Lubello, 'Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective' (2015) 20 Tilburg Law Review 14, 15.

[433] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union 2011 [2011/C 181/01] 1.

[434] See, in general, Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin UK 2011).

[435] 'Fire and Fury for Facebook' (*Interntational Financial Law Review*, 2018) <https://www.iflr.com/Article/3803223/Fire-and-fury-for-Facebook.html?ArticleId=3803223> accessed 14 September 2019.

overzealous legislators in check, as well as making sure private actors did not overstep the boundaries set by human rights standards.

4.8. How the Internet is Used to Undermine National Security

Expansion of the Internet goes hand in hand with the illicit purposes the technology may serve. The list of threats is numerous, and includes, *inter alia*, spreading malware, online harassment, digital blackmailing, cyberterrorism, and identity theft.[436] These diverse activities may be integrated under the broad term *cybercrime*, which Shipley and Bowker define as 'a criminal offence that has been created or made possible by the advent of technology, or a traditional crime that has been transformed by technology's use'.[437]

Owing to the constraints of this study, the present section will focus on illegal practices *vis-a-vis* national security concerns rather than on risks for private individuals.

The majority of terrorism-related crimes are currently committed with the use of digital technologies. Addressing this matter, a working group held by the United Nations Office on Drugs and Crime (UNODC) has named six types of activities where the Internet can be used to support terrorism:[438] these are propaganda, financing, training, planning, execution, and cyber-attacks.

Propaganda implies the dissemination of information to promote or justify acts of terrorism.[439] Digital tools have made it easier to spread violence-related information, which in earlier times could be shared with a somewhat limited audience via CDs, DVDs, and so on. Nowadays, with the capacities of the Internet, it has become simpler to reach a wide audience and to identify the most vulnerable target groups. Terrorist organisations address propaganda

---

[436] Todd G Shipley and Art Bowker, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace* (Newnes 2013) 21–38.
[437] ibid 2.
[438] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes.* (United Nations 2012) 3–12 <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>.
[439] ibid 4–5.

both to their potential recruiters and to their potential victims. When targeting victims, propaganda intensifies panic and vulnerability among the population, as opposed to propaganda aimed at potential recruiters, which is focused on finding new supporters, on radicalising, and on inciting to terrorism. Terrorists seek insecure marginalised groups that are experiencing social injustice, while minors are radicalised through popular multimedia formats such as games, cartoons, or music videos.

Financing is among the primary uses of the Internet for terrorist purposes. Donations for the purpose of financing attacks may be collected directly from supporters via money transfer websites, online stores, chats, and by other targeted means of communication. The Internet suggests many convenient services to transfer funds, such as Skype, PayPal, and so on. The same platforms can be used to raise money through card frauds, stock fraud, and identity theft. In addition, terrorists may collect money online under the pretext of running a charitable organisation. [440]

Training[441] entails spreading practical guides, videos, and other information on how to create firearms and explosives, and how to plan an attack or become a member of a terrorist organization. As for *planning*, a large amount of data is published every day worldwide, and can be used by terrorists to plan an attack. In particular, terrorists collect both logistical and sensitive information from social media accounts.[442]

Moreover, the Internet is a means to *execute* an attack. Terrorists may publish violent videos to spread panic in society. They can also establish communication with victims in order to threaten them and coordinate their moves.[443]

---

[440] ibid 7.
[441] ibid 8.
[442] ibid 10–11.
[443] ibid 11.

Cyber-attacks are similar to terrorist acts in their objective, which is to create chaos and panic, and they target core infrastructures such as networks, servers, and communication systems. Cyber-attacks include, *inter alia*, overloading the servers (phlooding), spreading viruses, hacking, and disclosing personal details.[444]

In its 2015 action plan on combating violent extremism, the UN General Assembly emphasised the role of the Internet in radicalising the young population.[445] Such influence is evident on the following grounds:

- Joining a radical organisation usually requires a personal acquaintance with one of the members; however, online tools provide more accessible means with regard to membership;[446]

- With the current level of Internet connectivity, young people form an unprecedented global community, and it has been exploited successfully by extremists;[447]

- Social media has facilitated the spreading of manipulative messages, especially among youth, while violent extremists have upgraded their use of digital and analogue media in a sophisticated manner.[448]

The role of the Internet in terrorism-related activities is also noted in national security agendas. The Royal Canadian Mounted police, for example, have stressed that 'the very nature of the Internet makes it an ideal venue for recruitment'.[449] In Australia, the Attorney General's Department also reports that the Internet is being used to spread violent messages and guidelines in order to create networks of individuals who condone violence, which can

[444] ibid.
[445] UN General Assembly Plan of Action to Prevent Violent Extremism (n 334).
[446] ibid 10.
[447] ibid 17.
[448] ibid 19.
[449] Royal Canadian Mounted Police (n 312) 10.

have consequences in real life.[450] The FBI experts note that terrorists use a large variety of tools to spread extremist ideologies: for example, 'password-protected jihadist Web sites, forums, blogs, social networking resources, and video-hosting services to professionally produced online English-language propaganda magazines'.[451]

Another set of security-related issues raised by Internet technologies may be attributed to big data capacities, which enables the identification of vulnerable groups in order to manipulate public opinion. The latter is exemplified by the recent Cambridge Analytica scandal,[452] which allegedly affected the results of Brexit and the 2016 US Elections. In addition, the previously mentioned electoral campaign of 2016 unleashed technology capacities in spreading disinformation and fake news. The role of the Russian 'trolls army' and cyber-attacks during the US presidential run has become a hot-button issue in recent years.[453]

Although the above-mentioned threats serve as striking examples of reasons to strengthen regulation of the Internet, limitations should ensure an appropriate balance with fundamental human rights, especially the right to freedom of expression.[454] This notion is developed in the following section.

---

[450] 'Preventing Violent Extremism and Radicalisation in Australia' (n 314) 14.
[451] Hunter and Heinke (n 313).
[452] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 14 June 2019.
[453] Jane Mayer, 'How Russia Helped Swing the Election for Trump' <https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump> accessed 18 August 2019; Dustin Volz and Alan Cullison, '"Putin Has Won": Mueller Report Details the Ways Russia Interfered in the 2016 Election' *Wall Street Journal* (19 April 2019) <https://www.wsj.com/articles/putin-has-won-mueller-report-details-the-ways-russia-interfered-in-the-2016-election-11555666201> accessed 18 August 2019; Rory Cellan-Jones, 'Russia "Meddled in All Big Social Media"' *BBC News* (17 December 2018) <https://www.bbc.com/news/technology-46590890> accessed 18 August 2019.
[454] See, in general, Oreste Pollicino and Oleg Soldatov, 'Judicial Balancing of Human Rights Online' in M Susi (ed), *Routledge Handbook on Digital Society* (Routledge 2019); Oreste Pollicino and Oleg Soldatov, 'Striking

4.9. Balancing Freedom of Expression with State Security Concerns

The regulation of digital communications occurs between two extremes. At one end are the proponents of making the Internet 'a world where one could talk and do business without worrying about state intervention',[455] and at the other are those who favour complete regulation of the online domain in a manner similar to, or even stricter than, regulation of the traditional media; those in favour of regulation call for licencing, supervision of content production, and complete user deanonymisation.[456] Following the initial years of Internet development,[457] the weaknesses of the most radical[458] arguments involving the presumed anarchic nature of the Internet have been exposed. Consequently, the larger issue is no longer whether it is possible to regulate the Internet; the issue now is how to do it.[459]

As Internet technology started gaining momentum in people's social life, states searched for ways to strengthen their role in online environments. Governments sought to control Internet activities under their jurisdiction, and indeed they have been obliged to do so.[460] Drawing from the case of *K.U. v Finland*,[461] states have a duty, under the ECHR, to protect the human rights of their citizens, both offline and online.

---

the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (2018) 19 German Law Journal 85.

[455] Henry Farrel, 'Why the Hidden Internet Can't Be a Libertarian Paradise' (*Aeon*, 20 February 2015) <https://aeon.co/essays/why-the-hidden-internet-can-t-be-a-libertarian-paradise> accessed 14 September 2019.

[456] *See* 'Predlozhenija Po Formirovaniju Dolgosrochnoj Programmy Razvitija Rossijskoj Chasti Informacionno-Kommunikacionnoj Seti "Internet" i Svjazannyh s Nej Otraslej Jekonomiki [Suggestions on Formulating the Long-Term Development Programme of the Russian Internet Sector and Related Branches of Economy]' <http://ири.рф/upload/iblock/2ee/2ee62c7a1204a3717e387869175d81e0.pdf> accessed 14 September 2019.

[457] The Internet entered the commercial phase in 1984–1989, and expanded into global networks during the 1990s when business and personal computers with different operating systems joined the universal network. *See* Raphael Cohen-Almagor, 'Internet History' (2011) 2 International Journal of Technoethics 45, 45–47.

[458] *See* John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 8 February 1996) <https://www.eff.org/cyberspace-independence> accessed 14 September 2019.

[459] *See* Pollicino and Bassini (n 440) 348.

[460] Benedek and Kettemann (n 409) 74.

[461] The court noted, *inter alia*, that National law should provide for privacy limitations for preventing crimes and protecting the rights and freedoms of others. See *KU v FINLAND* [2008] ECtHR 2872/02.

In 1998, Professor Goldsmith concluded that both cyberspace and ordinary transactions involve people in real space transacting with other people in real space, which sometimes results in real- world harm.[462] In pursuit of solutions to curb cybercrime, the legislative approach is usually to engage in a proportionality analysis involving the right 'to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'[463] and other societal interests.[464] The balance struck differs dramatically across different jurisdictions.[465] Europe presents a perfect illustration of how varied Internet regulation can be within a certain geographic space, given the differences between approaches prevailing in the EU and practices of the recent and widely discussed Russian legislative package regulating the online domain, enacted by the Sixth Convocation of the Russian Parliament (2011-2016) − the State Duma.

[462] *See* Jack L Goldsmith, 'Against Cyberanarchy' (1998) 65 The University of Chicago Law Review 1199, 1200.
[463] *See* European Convention on Human Rights (n 292) Art. 10.(defining freedom of expression).
[464] *See Ahmet Yildirim v Turkey* [2012] ECtHR 3111/10 [8–9].
[465] Erik Bleich, 'Freedom of Expression versus Racist Hate Speech: Explaining Differences between High Court Regulations in the USA and Europe' (2013) 40 Journal of Ethnic and Migration Studies 283, 283.

5. Expression Online: Best Practices and Existing Frameworks in the 'Old' Democracies

The collapse of the Soviet Union was a period of dramatic changes in the world order. The former republics had not only to rebuild their national identities but also to search for a new political system, as communism had lost its significance as a state order system.[466] Such a view is simplified to an extent, however, as in Russia and Central Asian states, the transformation thus far has resulted in the establishment of authoritarian regimes, whereas countries like Georgia and Ukraine are currently in transition.[467] Developments *vis-à-vis* freedom of expression are represented accordingly in the mentioned sub-regions.

It should be noted that the period of transformation itself is a complex issue. Countries in transition are usually experiencing the double processes of political and economic liberalisation after the breaking down of the autocratic order. These processes imply uncertainty and ineffective political institutions, as the new political and administrative state institutions have not yet gained full political legitimacy and operational capacity.[468] A number of South American and post-Soviet countries can be or have been categorised as countries in transition.

In this work, the author opposes online regulation in post-Soviet countries with regard to those established in 'old' democracies: namely, the countries that were continuously democratic prior to the 1990s. Specifically, the author will draw from European and selective American practices as a benchmark to evaluate case studies from the region under scrutiny.

---

[466] Bruce Parrott, 'Perspectives on Postcommunist Democratization' in Karen Dawisha and Bruce Parrott (eds), *Democratic changes and authoritarian reactions in Russia, Ukraine, Belarus and Moldova*, vol 3 (Cambridge University Press 1997).

[467] 'Nations in Transit 2018: Confronting Illiberalism' (11 April 2018) <https://freedomhouse.org/report/nations-transit/nations-transit-2018> accessed 30 August 2019.

[468] Michael Heller and Merritt B Fox, *Corporate Governance Lessons from Transition Economy Reforms* (Princeton University Press 2006).

In addition, the author will refer to recommendations of intergovernmental organisations, relevant practices developed in international law, and global trends in online regulation.

To set the stage, although the Internet in the world was virtually unregulated at first, the growing list of illegal activities online has given rise to mechanisms to identify liable parties with a view to holding them criminally or otherwise accountable for their actions.[469] This is nothing new, and the current regulation of the online domain does not present any unsolvable problems to legislators across the world. At present, in the worldwide context, state authorities and private companies tend to respond to cybercrime using a combination of soft law and hard law instruments.[470]

In Europe, for instance, hard law instruments include EU-level legislation − applicable solely in the 28 EU member states − as well as the European Convention of Human Rights − applicable throughout the 47 Council of Europe member states. The provisions of the latter concerning freedom of expression on the Internet have been interpreted by the European Court of Human Rights − a transnational judicial body that hears applications alleging that one or more of the Council of Europe member states has breached one or more of the human rights provisions set out in the Convention and its protocols. Both EU-wide and Council-wide, hard law instruments recognise the rights to privacy of communication and to freedom of expression.

These instruments can be divided into two categories: 1) the legal obligation of Internet Service Providers (ISPs) to report and/or block certain categories of content and 2)

[469] Jack M Balkin, 'The Future of Free Expression in a Digital Age' (2008) 36 Pepp. L. Rev. 427, 434–435.

[470] The primary legal instruments regulating the online domain in the territory of Europe include the Council of Europe legal instruments (including but not limited to the 2001 Convention on Cybercrime with its Additional Protocol; the 2007 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse) and the European Union instruments (including but not limited to Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce in the Internal Market; and Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data) as well as national legislation.

criminalising certain activities on the part of Internet users. Additionally, the EU, with a few exceptions, has not implemented content regulation, and member states are therefore free to determine their own policies, provided that they conform to Article 10 of the European Convention on Human Rights.[471] Generally speaking, the grounds for blocking online content, and, in certain cases, holding its disseminators liable, include the protection of national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, and prevention of the disclosure of information received in confidence.[472] In older European democracies, it is only possible to block and take down illegal content on the Internet upon the issuance of case-by-case injunctions by courts, and, in fewer cases, upon decisions of other State authorities.[473]

In turn, soft law also includes EU initiatives such as the 2016 Code of Conduct on illegal online hate speech that was developed in cooperation with the European Commission,[474] the Council of Europe-wide tools such as the guide to the human rights of Internet users,[475] and the codes of conduct and terms of service of ISPs and other intermediaries.[476]

---

[471] For a more elaborate presentation, see Oreste Pollicino and Marco Bassini, 'Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis' in A. Savin and J. Trzaskowski (eds), *Research Handbook on EU Internet Law* (2014) 541.

[472] *See* 'Filtering, Blocking and Take-down of Illegal Content on the Internet' (*Council of Europe/Conseil de l'Europe*, 20 December 2015) <https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet> accessed 3 August 2019.

[473] ibid.

[474] *See* 'European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech' (*European Commission*, 31 May 2016) <https://europa.eu/rapid/press-release_IP-16-1937_en.htm> accessed 3 August 2019.

[475] *See* 'Internet Users' Rights' (*Council of Europe/Conseil de l'Europe*, 16 April 2014) <https://www.coe.int/en/web/freedom-expression/internet-users-rights> accessed 3 August 2019.

[476] *See* Damian Tambini, Danilo Leonardi and Chris Marsden, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (Routledge 2007) 28–49, 112–189.

At the soft law level, in Europe the human rights of Internet users recognised by the Council of Europe[477] include the right to non-discriminatory access to the Internet; the right to seek, receive, and impart information and ideas of one's choice without interference and regardless of frontiers; the right to assemble peacefully and to associate with others using the Internet; and the right to a private and family life on the Internet, which includes the protection of personal data and respect for the confidentiality of correspondence and communication.

It should be reiterated that, at times, some of the rights recognised in hard and soft law, as is the case with other human rights,[478] might be temporarily or permanently restricted in order to prevent cybercriminal activities. The taxonomy of e-crime is varied, and the most important categories of criminal activities online can be summed up as follows: a) crimes where the computer, network, or electronic device is the target of criminal activity: for example, disrupting computer services; b) content violation offences: for example, unauthorised possession of military secrets, intellectual property offences; c) online fraud; and d) improper use of telecommunications, such as cyberstalking, spamming, and conspiracy to undertake harmful or criminal activity.[479]

State security concerns stemming from a terrorist[480] threat seem to be prominent on national and international agendas these days, and are a reason *de jure* for many governments

[477] 'Internet Users' Rights' (n 475).

[478] For instance, the rights and freedoms guaranteed by Articles 8 (right to respect for private and family life), 9 (freedom of thought, conscience, and religion), 10 (freedom of expression), and 11 (freedom of assembly and association) of the European Convention on Human Rights are qualified, and each Article contains a limitation clause. No restrictions on these rights are permitted other than those expressly listed, and such restrictions must have a legitimate aim.

[479] *See* David Simms and Solange Ghernaouti, 'Report on Taxonomy and Evaluation of Existing Inventories' (European Union E-Crime Project 2014) <www.ecrime-project.eu/wp-content/uploads/2015/02/E-Crime-Deliverable-2-1-20141128_FINAL.pdf> accessed 8 December 2017.

[480] For the purposes of this research, this concept is defined as 'the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious or social goal through fear, coercion or intimidation'. Gary LaFree and Laura Dugan, 'Introducing the Global Terrorism Database' (2007) 19 Terrorism and Political Violence 181, 184.

to set limitations on online expression. In the recent words of Věra Jourová, EU Commissioner for Justice, Consumers, and Gender Equality,

> *the recent terror attacks have reminded us of the urgent need to address illegal online hate speech. Social media is unfortunately one of the tools that terrorist groups use to radicalise young people*.[481]

In exploring the question of terrorism-related speech online, the dichotomy of 'positive' and 'negative' measures of curbing illegal behaviour in the digital world may be introduced. 'Positive' measures refer to those online initiatives that seek to make an impact through digital engagement and education and the provision of counter-narratives, while 'negative' measures describe 'those approaches that advocate for, or result in, the deletion or restriction of violent extremist online content and/or the legal sanctioning of its online purveyors or users'.[482]

In presenting specific spheres of regulation, the author will draw parallels with the following areas of legislative activity in the post-Soviet region:

- modalities for removal of content;
- online anonymity (including the connected question of intermediary liability);
- data protection and retention policies;
- data nationalism.

[481] 'European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech' (n 474).
[482] Clive Walker and Maura Conway, 'Online Terrorism and Online Laws' (2015) 8 Dynamics of Asymmetric Conflict 156, 156.

5.1. Modalities for Removal of Content

In Section 4, *Online Expression and National Security: Concepts and Definitions*, the author highlights fundamental challenges with respect to the regulations of online communication, which concern both the specific nature of the Internet and the problem with defining key terms of illegal content: for instance, 'terrorism' and 'extremism'. The present section presents policy recommendations regarding the latter challenges, aimed at covering two fundamental questions: 1) which categories of content should be legitimately blocked and 2) how should the states carry out Internet filtering.

At the European level, online content is divided into 'illegal' and 'harmful'. As early as 1996, the European Commission stressed that, 'These different categories of content pose radically different issues of principle, and call for very different legal and technological responses'.[483] Whereas illegal content is a subject of criminal prosecution in nation states, harmful content may be offensive and undesirable for some social groups, but it is not usually criminalised under national laws.[484]

While most of the states adopt policies to prevent the dissemination of certain categories of online content, the definition of what is illegal or harmful (but legal) varies greatly throughout jurisdictions.[485] Cultural, religious, and historical peculiarities play an important role in what expression is outlawed. In Germany, Austria and France, for example, denial of the Jewish Holocaust entails criminal liability; however, countries with different historical roots may decide not to penalise such an expression of opinion.[486] Therefore, even though the governments express a major concern regarding the dissemination of terrorist propaganda, hate speech, and disinformation on the Internet, their approaches to labelling

[483] EU Commission, Illegal and harmful content on the internet 1996 [COM (96) 487 final] 10.
[484] Yaman Akdeniz, 'To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression' (2010) 26 Computer Law & Security Review 260.
[485] EU Commission Illegal and harmful content on the internet (n 483).
[486] Akdeniz (n 484).

such content have fundamental differences. Such diversity brings complexity to the harmonisation of legal practices at the international level.[487]

Drawing on regional complexities, intergovernmental organisations generally reserve the right of the states to decide which categories of content should be banned. Nonetheless, several leading principles regarding Internet filtration have been developed on an international level.

The first grounding rule suggests that 'the same rights that people have offline must also be protected online,' as established in the *UN Human Rights Council Resolution No. A/HRC/20/8* of 5 July 2012.[488] The Resolution takes particular note of the right to freedom of expression, which should be respected regardless of national frontiers and via any kind of media.

In accordance with this principle, Frank La Rue, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, stressed that similarly to offline content, any restriction on online content should be imposed through a three-step test: (1) it must be provided by law to follow the principles of predictability and transparency; (2) it must pursue one of the purposes set out in Article 19 of the ICCPR, whether to protect the rights or reputations of others, national security, or public health and morals (principle of legitimacy); and (3) it must be proven as a necessary and the least restrictive means required to achieve the alleged purpose (principle of proportionality).[489] Similar criteria –

[487] Yaman Akdeniz, *Media Freedom on the Internet: An OSCE Guidebook* (OSCE Representative on Freedom of the Media 2016) 31.
[488] Resolution of the Human Rights Council 'On The promotion, protection and enjoyment of human rights on the Internet' (n 409).
[489] Frank La Rue Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (n 424).

transparency, legitimacy, and proportionality − are followed by the European Court of Human Rights.[490]

At the EU-wide level, Directive 2000/31/EC includes a mild incentive for ISPs to take down illegal material voluntarily. This Directive states that ISPs have limited liability only when they do not have actual knowledge of illegal activity or information. And the damages will be limited if they are not aware of the facts or circumstances based on which the illegal activity or information is apparent. At the same time, ISPs are not under a general obligation to monitor the information that they transmit or store, nor are they under a general obligation to actively seek facts or circumstances indicating illegal activity.

Most commonly,[491] a court order is necessary for unconditional blocking, although, as the UK example demonstrates, self-regulation arrangements might also be a viable solution. In the UK, material that encourages terrorism can generally be placed on 'blacklists' without court orders. According to a study commissioned by the Council of Europe,[492] in the UK, the watchdogs in charge of deciding which content to take down include various governmental agencies in charge of Internet-related offences. For instance, the Counter Terrorism Internet Referral Unit, acting in accordance with the Terrorism Act 2006, compiles the blacklist of URLs for material hosted outside of the UK that would give rise to criminal liability. The Police Intellectual Property Crime Unit is responsible for decisions to remove content or to report these offences.

Regardless of the hosting location, since 2013, the removal of unlawful terrorist content has been achieved through informal contact between the police and ISPs, and it has

---

[490] Nils Muižnieks, 'Arbitrary Internet Blocking Jeopardises Freedom of Expression' (*Commissioner for Human Rights*, 26 September 2017) <https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/arbitrary-internet-blocking-jeopardises-freedom-of-expression> accessed 10 July 2019.

[491] *See* Nigel Cory, 'The Worst Innovation Mercantilist Policies of 2016' [2017] ITIF <http://www2.itif.org/2017-worst-innovation-mercantilist-policies.pdf>; 'Internet Users' Rights' (n 475) n 15.

[492] 'Filtering, Blocking and Take-down of Illegal Content on the Internet' (n 472).

never been necessary to use formal powers under the Terrorism Act 2006. It is noted further that in the UK there are only two areas that require statutory notice and removal procedures for the scrubbing of illegal Internet content: The first, in relation to material that constitutes offences under the Terrorism Act 2006, and the second, in relation to the Defamation Act 2013.

Overseas, U.S. authorities are very reluctant to block illegal content on the Internet, given the strong protections afforded to freedom of speech under the First Amendment to the U.S. Constitution.[493] In the absence of legal regulation to remove offensive material, authorities rely on the cooperation of online platforms, whose abuse policies allow the removal of accounts flagged for promoting terrorism.[494] The 1996 Communications Decency Act and the 1998 Child Online Protection Act, which were the legislature's attempts to counter the spread of indecent information online, were struck down by U.S. courts.[495]

5.2. Online Anonymity

When it comes to the question of online anonymity, it is observed that, both in the EU and the U.S., the anonymity of Internet users remains protected by default for those who do not wish to disclose their identity. Nevertheless, the right to privacy must often be reconciled with conflicting policy objectives, such as the fight against illegal or harmful content. The European Commission's long-held view on this issue, generally supported by the case law of the European Court of Human Rights,[496] is that 'the ability of governments and public authorities to restrict the rights of individuals and monitor potentially unlawful behaviour should be no greater on the Internet than it is in the outside, off-line world'.[497] The

[493] *See* United Nations Office on Drugs and Crime (n 438) 95–96.
[494] *See* Peter R Neumann, *Countering Online Radicalization in America* (Bipartisan Policy Center 2012).
[495] Pollicino and Bassini (n 471) 517–520.
[496] *See in general,* 'Internet: Case-Law of the European Court of Human Rights' (n 402).
[497] 'Recommendation 3/97. Anonymity on the Internet' (Working Party, European Commission 1997) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_en.pdf>

Ministerial Declaration of the Ministerial Conference in Bonn on Global Information Networks, July 6-8, 1997, declared a formula that continues to be 'where the user can choose to remain anonymous off-line, that choice should also be available on-line'.[498]

Meanwhile, in the recent case, *Delfi AS* v *Estonia*, the European Court of Human Rights supported the proposition of holding online intermediaries responsible for the content published by third parties.[499] In this case, the Court decided that the civil liability imposed by the Estonian courts on *Delfi*, an Internet news portal and an applicant in the case, for defamatory comments posted by anonymous readers below one of *Delfi*'s online articles was compatible with guarantees provided by the Convention, and did not constitute a disproportionate restriction on the applicant company's right to freedom of expression. This decision is considered to push online intermediaries towards a strategy of gradual deanonymisation of online users that actively participate in online discussion.

The outcome of this case has been criticised[500] for weakening freedom of expression on the Internet: given the Court's high legitimacy,[501] its findings may be translated into the Council of Europe member-state legislation and interpretative legal practices by the national courts. It can also be argued that one of the most obvious responses of online intermediaries to protect themselves from potential liability is to introduce screening and pre-moderation of user-created commentaries. This, in turn, could undo one of the maxims of online communication: today, to increase the flow of Internet traffic and site search ranking, Internet portal managers are encouraging readers to leave comments and are avoiding moderation. On

---

accessed 16 June 2019.

[498] European Union Ministers Bonn Declaration 1997.

[499] *See Delfi AS v Estonia* (n 404).

[500] Tatiana-Eleni Synodinou, 'Intermediaries' Liability for Online Copyright Infringement in the EU: Evolutions and Confusions' (2015) 31 Computer Law & Security Review 57.

[501] Basak Cali, Anne Koch and Nicola Bruch, 'The Legitimacy of Human Rights Courts: A Grounded Interpretivist Analysis of the European Court of Human Rights' (2013) 35 Hum. Rts. Q. 955.

the contrary, as Halligan and Shah[502] warn, such moderation is an extra step in the process that creates just enough friction to ensure that meaningful conversations between online users cannot really take place.

An extra layer of complexity is added by the fact that many online intermediaries do not host and manage their website comment sections themselves. Instead, they outsource this activity to comment-hosting services for websites and online communities, such as 'Disqus'.[503] This further poses a plethora of jurisdictional issues and unresolved problems.

Of course, it is premature to draw conclusions from *Delfi*, as the mechanisms for such deanonymisation − for example, updating terms of service of online intermediaries and other repercussions of this judgement − need to be analysed further, based on subsequent case law developments.[504]

The United States Supreme Court has ruled that the right to speak anonymously is protected by the First Amendment, because anonymity is 'a shield from the tyranny of the majority' that protects 'unpopular individuals' from retaliation at the hands of an intolerant society.[505]

It is obvious that in response to a wider adoption of tools that make discovery of the real identity of a given user more difficult, such as data encryption, virtual private networks,[506] and onion routing,[507] more effective monitoring tools are being introduced by

---

[502] Brian Halligan and Dharmesh Shah, *Inbound Marketing.: Get Found Using Google, Social Media, and Blogs* (John Wiley & Sons 2009) 43–44.

[503] See Hasan Al Maruf and others, 'Human Behaviour in Different Social Medias: A Case Study of Twitter and Disqus', *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (IEEE 2015)., among other authorities

[504] *See Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* [2016] ECtHR (Fouth Section) 22947/13.

[505] *Mcintyre v Ohio Elections Commission* [1995] US Supreme Court 514 US 334.

[506] A Virtual Private Network extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. *See* Kat Aoki, 'How to Hide Your Identity and Data on the Web With a VPN' (*Lifewire*, 14 October 2016) <https://www.lifewire.com/what-is-a-vpn-2377977> accessed 3 August 2019.

investigative authorities. In particular, deep packet inspection (DPI), a technology for scanning and analysing Internet traffic and making decisions about how to handle it in real time, has emerged.[508] Some countries are choosing to enact mandatory key disclosure legislation, which requires individuals to surrender their cryptographic keys to law enforcement authorities.[509]

5.3. Data Protection and Data Retention

The post-9/11 era 'can be characterised by the desire and ability of governments to develop a global mass surveillance system, largely unseen and until recently unsuspected', and 'a common trend can be discerned whereby governments monitor the communications and online behavior of the vast majority of ordinary citizens'.[510] Whereas the European Court of Human Rights has often extended a margin of appreciation to Member States when privacy rights have clashed with national security concerns,[511] at the EU level, the attempt to codify data retention rules in an overly wide manner was denied by the European Court of Justice. The events unfolded as follows. The 2006 EU Data Retention Directive[512] prescribed the storage of EU citizens' telecommunications metadata for a minimum of 6 months and at most 24 months, and allowed investigative authorities access to details such as IP addresses and times of use with regard to every email, phone call, and text message sent or received,

---

[507] The most well-known application for relaying onions is *Tor*, dedicated software that protects a user by bouncing his/her communications around a distributed network of relays run by volunteers all around the world, thereby preventing third parties from monitoring a user's Internet connection and learning what sites he/she visits, as well as preventing the sites from learning the user's physical location. *See* 'Tor FAQ' (*Tor Project*) <https://2019.www.torproject.org/docs/faq> accessed 3 August 2019.

[508] *See* Ebenezer Duah, 'Internet Service Providers' Monitoring Obligations: Recent Developments' (2012) 6 Masaryk UJL & Tech. 207, 208.

[509] *See* Regulation of Investigatory Powers Act 2000 (Eng.), and subsequent amendments.

[510] Vedaschi and Lubello (n 432) 15.

[511] *See* Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2015) 28 Harv. Hum. Rts. J. 65, 69.

[512] *See* Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC 2006 [2006/24/EC].

conditional upon court approval. The retention of data was used to serve the purpose of preventing, investigating, detecting, and prosecuting serious crimes, such as organised crime and terrorism. On April 8, 2014, the Court of Justice of the European Union declared the Directive invalid on the grounds that interference with the fundamental rights to respect for privacy and the protection of personal data was not limited to strictly necessary materials.[513] In December 2016, the Court further elaborated that EU law precludes national legislation that prescribes the general and indiscriminate retention of data.[514] Following these developments, it appears that the European Court of Human Rights supported the conclusion concerning the illegality of indiscriminate data collection and retention.[515] Unlike the EU Data Retention Directive, the United States does not have ISP-level mandatory data retention laws.[516]

5.4. Data Nationalism

A growing number of policymakers in Europe seem to subscribe to the 'data nationalism'' view: the belief that data are more secure when stored within a country's borders,[517] which leads to the emergence of various countries' policies that would require a certain body of data to be stored domestically. Driven by concerns over privacy, security, surveillance, and law enforcement, some governments are erecting borders in cyberspace. Although the first generation of Internet border controls sought to keep information out of a country − for example, copyright-infringing material − the new generation of controls seeks to keep all data about individuals within a country, citing foreign surveillance as an

[513] *See Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] CJEU C-293/12 and C-594/12.
[514] *See Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] CJEU C-203/15 and C-698/15.
[515] See *Roman Zakharov v Russia* [2015] ECtHR 47143/06.
[516] See Christina Akrivopoulou and Athanasios Psygkas, *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices* (IGI Global 2011) 257.
[517] Daniel Castro, 'The False Promise of Data Nationalism' [2013] Information Technology and Innovation Foundation.

argument.[518] Similar to real-world border controls, data nationalism policies can be seen from two perspectives: restrictive, where a country seeks to use data nationalism to subject stored data to overly restrictive legislation, and protective, where a country uses data nationalism to protect unsuspecting users from having their data stored in countries with either very lax or very intrusive policies. Some researchers argue that just as economic nationalism inevitably leads to lower productivity for firms and higher costs for consumers, data nationalism will similarly lead to poor economic outcomes. [519]

When it comes to the EU, there are virtually no borders between individual EU member states regarding the cross-border data flow. Nevertheless, General Data Protection Regulation 2016/679 entered into force on May 25, 2018, and will allow companies to transfer data outside the European Union, only if appropriate safeguards are in place to ensure a level of protection for the rights of data subjects equal to that envisaged by the General Data Protection Regulation. Many countries, such as Germany and France, are at the centre of efforts to force companies to store data only in the European Union or even in-country, such as through a 'Bundescloud' (a cloud for government data) in Germany, where, on July 1, 2017, a law requiring local data storage for telecommunications metadata entered into force.[520]

[518] *See* Anupam Chander and Uyên P Lê, 'Data Nationalism' (2014) 64 Emory LJ 677, 679.
[519] Castro (n 517).
[520] Cory (n 491).

6. Post-Soviet Region: Case Studies of Online Regulation

Several reasons exist for the cross-fertilisation involving legal norms and practices across the region. It starts with the commonality of the character of local political regimes; irrespective of whether they are authoritarian, semi-authoritarian, or troubled democracies, they share a similar desire to maintain their political dominance.[521] This peculiarity is captured in Section 3.2 on *Regional authoritarianism*. At the heart of adopting copycat legislation is a similar fear on the part of ruling elites regarding popular protests, which in recent decades have taken place in many parts of the world. The finding is based on previous observations: namely, '*The common space of neo-authoritarianism in post-Soviet Eurasia'* – which covered a similar replication of restrictive laws on public gatherings during Ukraine's Euromaidan protests in 2014[522] – and on *'Freedom of media under attack across the former Soviet Union'* – which stressed that the climate for free expression in the FSU deteriorated even further after the revolution in Ukraine.[523] This study supports evidence from the previous investigations with respect to online regulations.

Another possible explanation involves a universal trend of cross-fertilisation in technology-related legislation.[524] By way of illustration, the European judicial approach concerning jurisdiction on the withdrawal of information had a spillover effect after the European Court of Justice announced the Google Spain decision.[525] It should be noted that

[521] Hug (n 205) 3.
[522] Oleg Antonov and Artem Galushko, 'The common space of neo-authoritarianism in post-Soviet Eurasia' (*Baltic Worlds*, 5 March 2019) <http://balticworlds.com/the-common-space-of-neo-authoritarianism-in-post-soviet-eurasia/> accessed 16 July 2019.
[523] Katie Morris, 'Freedom of the Media under Attack across the Former Soviet Union' (*The Foreign Policy Centre*, 24 May 2016) <https://fpc.org.uk/freedom-media-attack-across-former-soviet-union/> accessed 10 July 2019.
[524] Pollicino and Soldatov, 'Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (n 454).
[525] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* [2014] CJEU C-131/12; Krystyna Kowalik-Bańczyk and Oreste Pollicino, 'Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information' (2016) 17 German Law Journal 315.

most of the sections below reflect the urgent global topics involving online regulation. This list includes a variety of issues such as fake news, data protection, cybercrimes, and many others. Therefore, the author suggests that legislators across the former Soviet Union are prompted by a mix of different influences, not only from neighbouring countries but also following certain global trends. In reality, amended online regulations commonly fail to meet international legal requirements, and copy 'worst practice' from other jurisdictions.[526]

It would be erroneous to assume that Russia is the 'mastermind' of all the repressive online legislation in the region. Rather, its role rests in maintaining a conservative regional values agenda, which seems attractive to other authoritarian regimes, and in providing new legislative ideas for neighbouring countries. In spite of the fact that there might be some support for restrictive regulations through regional entities and mutual agreements, the regimes under scrutiny need no encouragement to establish greater state control. As Hug usefully noted, countries such as Uzbekistan or Turkmenistan 'need no direction from Russia or indeed China to clamp down on dissent but remain open to new methods of how to do so'.[527]

It should be noted, however, that not all sub-regional groups from the post-Soviet states be categorised as 'authoritarian'. Whereas the majority of former Soviet republics remained committed to an authoritarian model,[528] several states – such as Georgia or Ukraine – struggled down the path of democratisation.[529] Baltic states, exemplified in this thesis by Estonia, represent an important exception in comparison to the analysed countries. As countries became full EU members, they integrated their regulations into common *acquis communautaire* framework, including the legal instruments dealing with fundamental rights

[526] Hug (n 205).
[527] ibid.
[528] ibid 5.
[529] 'Eurasia' (n 25).

and freedoms, inter alia the protection of privacy, freedom of expression and e-commerce. Following the dissolution of the Soviet Union, this sub-regional group took a consistent step towards democratic development.[530]

The following section summarises the peculiarities of online regulation in the post-Soviet region, and, most notably, the similar replications of legal initiatives with respect to state security concerns.

6.1. Legitimising Limitations to Freedom of Expression in the Post-Soviet Region: State Security Concerns

6.1.1. Anti-Extremism and Anti-Terrorism Legislation

As a result of recurrent terrorist attacks over the past few decades, many states are facing a need to deter and to combat future threats. However, the implementation of anti-terrorism and anti-extremism legislation poses considerable risks to fundamental civil liberties, including freedom of expression and freedom of the media. The misuse and an overdose of anti-terror legislation are now demonstrating a trend that reaches beyond post-Soviet space. Recently, the Council of Europe Commissioner for Human Rights, Dunja Mijatović, expressed concern with respect to the tendency to misuse anti-terror legislation across Europe.[531] According to her statement, 'states are often tempted to restrict fundamental freedoms for the sake of fighting it and preventing further attacks'. Along similar lines, the OSCE stressed that broad notions of national security may pose a threat both to freedom of expression and the media.[532]

---

[530] Fagan and Kopecký (n 122) 113–117.

[531] 'Misuse of Anti-Terror Legislation Threatens Freedom of Expression' (*The Council of Europe Commissioner for Human Rights*, 12 April 2018) <https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/misuse-of-anti-terror-legislation-threatens-freedom-of-expression> accessed 14 September 2019.

[532] 'Joint Declaration on Media Independence and Diversity in the Digital Age' (*OSCE*, 2 May 2018) <https://www.osce.org/representative-on-freedom-of-media/379351> accessed 14 September 2019.

Unbalanced and ill-fitting anti-terrorism practices are even more evident within the FSU region, owing to the diverse ethnic composition and long-term historical tradition of authoritarian governments.[533] Behind the smoke screen of 'protecting' citizens, governments are reinforcing legal frameworks that grant regulative authorities almost unlimited power to combat any unwanted expression. Therefore, any critical expression *vis-à-vis* a leading regime can easily be interpreted as 'extremist', 'a threat to national security', or 'inciting hatred and terrorism'. This is particularly the case with respect to the opposition media outlets. For instance, in 2018, Belarus authorities targeted Charter 97, the most popular news website, which was backed by the opposition and human rights organisations, and had always been critical of the authorities. The media was accused of disseminating 'extremist' content and harming Belarusian national interests. This was not the first case of site blocking; in fact, due to the recurrent pressure, the site had moved its headquarters to Poland in 2011. Reporters Without Borders condemned the banning of independent media.[534]

Major issues of concern with respect to existing legal frameworks are related to 1) broad provisions and vague definitions of the term 'extremism' or other terms[535] and to 2) disproportional restrictions on freedom of expression.[536]

---

[533] Pollicino and Soldatov, 'Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (n 454).

[534] See 'Blocking of Leading Belarusian News Website Seen as Test for EU' (*RSF*, 30 January 2018) <https://rsf.org/en/news/blocking-leading-belarusian-news-website-seen-test-eu> accessed 25 June 2019. Similarly, legislation on extremism provided the grounds for Russian authorities to block oppositional websites Grani.ru, Kasparov.ru, Ej.ru, Navalny. livejournal.com. See Maria Kravchenko, 'Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2014' (*SOVA Center*, 2015) <http://www.sova-center.ru/en/misuse/reports-analyses/2015/06/d32083> accessed 14 September 2019.

[535] Analysing Kyrgyz Law on Extremist activity, Article 19 noted an overly broad definition of extremism, which would allow the government to target legitimate speech. The analysis expressed the concern that 'Law might be used to crack down on NGOs criticising or merely holding views different from those of the government'. See 'Kyrgyzstan: Law on Countering Extremist Activity' (Article 19 2015) 10 <https://www.article19.org/data/files/medialibrary/38221/Kyrgyzstan-Extremism-LA-Final.pdf> accessed 25 June 2019. The Belarusian Association of Journalists noted the threat of a broad interpretation of 'extremist' in the legislation: See 'Mass Media in Belarus: E-Newstseller' (BAJ 2014) 4 <https://baj.by/sites/default/files/analytics/files/3372014_mass_media_in_belarus_en.pdf>. A similar weakness in the legislation is noted in Russia, Uzbekistan, and Kyrgyzstan.

An example of overly broad terminology is given in the Venice Commission's assessment of the 2002 Federal Law of the Russian Federation 'On Combating Extremist Activity'.[537] The Venice Commission concluded that:

> *The Extremism Law, on account of its broad and imprecise wording, particularly insofar as the "basic notions" defined by the Law – such as the definition of "extremism", "extremist actions", "extremist organisations" or "extremist materials" – are concerned, gives too wide discretion in its interpretation and application, thus leading to arbitrariness […]. The activities defined by the Law as extremist and enabling the authorities to issue preventive and corrective measures do not all contain an element of violence and are not all defined with sufficient precision to allow an individual to regulate his or her conduct or the activities of an organisation so as to avoid the application of such measures.* [538]

This evaluation raises concerns that arbitrary blocking may be a strategy used by the government to silence voices of opposition.[539]

---

[536] For instance, in Kyrgyzstan, the Prosecutor General Office can demand the dissolution of NGOs that conduct 'extremist activities' 'Kyrgyzstan: Law on Countering Extremist Activity' (n 535). In Russia, the General Prosecutor may order, without court approval, the shutting down of websites 'suspected of extremism',' calling for illegal meetings', 'inciting hatred', and 'violating the established order'. See Section 6.2.2, *'Mechanism to block websites without judicial approval'*.

[537] Federal Law 'On Combating Extremist Activity' 2002 [114-FZ].

[538] Venice Commission, Opinion on the Federal Law on Combating Extremist Activity of the Russian Federation 2012 [CDL-AD(2012)016]; Oleg Soldatov, 'The Russian VPN ban: another round in the battle for a free Internet' (*European Centre for Press and Media Freedom*, 20 September 2017) <https://www.rcmediafreedom.eu/Tools/Legal-Resources/The-Russian-VPN-ban-another-round-in-the-battle-for-a-free-Internet> accessed 16 July 2019.

[539] Soldatov, 'The Russian VPN ban' (n 538).

Freedom House pointed to similar patterns in the over-use of anti-extremism legislation in Russia,[540] Belarus,[541] Kazakhstan,[542] Kyrgyzstan,[543] and Uzbekistan.[544] A notable shift occurred in 2013-2014, following the Revolution of Dignity in Ukraine.[545] A range of studies highlighted the synchronic replication of restrictive laws on public gatherings in Russia and Central Asian republics after the Ukrainian protests.[546] This research revealed that authoritarian leaders had responded to the oppositional events with tougher anti-extremism legislation, both to prevent the risk of separatism in ethnic minority regions and to ensure that the leading regime was able to hold on to power.

At the end of 2013, President Putin signed Federal Law No. 398-FZ, known as 'Lugovoy's Law'. The legislative amendments authorised the General Prosecutor's Office to execute the extrajudicial blocking of websites if they were 'suspected of extremism', 'calling for illegal meetings', 'inciting hatred', and undertaking 'any other actions' 'violating the established order'.[547]

The reasons at the heart of the implementation of 'Lugovoy's Law' seem ambivalent. On the one hand, the legislative package may be viewed as a sincere effort to combat

---

[540] 'Freedom on the Net 2018: Russia' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/russia> accessed 23 June 2019.
[541] 'Freedom on the Net 2018: Belarus' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/belarus> accessed 25 June 2019.
[542] 'Freedom on the Net 2018: Kazakhstan' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/kazakhstan> accessed 25 June 2019.
[543] 'Freedom on the Net 2018: Kyrgyzstan' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/kyrgyzstan> accessed 25 June 2019.
[544] 'Freedom on the Net 2018: Uzbekistan' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/uzbekistan> accessed 25 June 2019.
[545] In December 2013, the former Ukrainian government under Victor Yanukovych refused to sign the EU Association Agreement, and brutally suppressed pro-European protests. This provoked revolutionary events in Ukraine, and the overthrow of the government. The change of regime ignited the conflict between Russia and Ukraine. See under Section 3.2.4, *'Ukraine: Crimea and Donbas'*.
The authoritarian governments responded with fear to the possibility of social protest; therefore, to prevent similar events in their own countries, they introduced harsher legislative measures.
[546] Antonov and Galushko (n 522).
[547] 'Russian Efforts At Internet Censorship' (*Radio Free Europe/Radio Liberty*, 13 February 2019) <https://www.rferl.org/a/russian-efforts-at-internet-censorship/29768034.html> accessed 21 June 2019.

extremism and terrorism. On the other hand, it may be seen as a sign that the authoritarian government targeted the last medium for free expression under the smoke screen of national security.[548]

The amendments targeted a number of Ukrainian websites, as their views were directly in opposition to the official policy of the Kremlin. The list included media such as Liga, Korrespondent, Bigmir, and Krym.Realii.[549] The Ukrainian media were blocked in Russia for publishing a quote from the leader of the Crimean Tatar national movement, Refat Chubarov, who stressed that the annexed peninsula should be returned to Ukraine.[550] In March 2014, the law allowed the blocking of the opposition media outlets Grani.ru, Kasparov.ru, Ej.ru, and Navalny.livejournal.com, on the grounds that they were 'calling for unlawful activity'.[551]

At the culmination of the Euromaidan events in January 2014, the Administration of the incumbent Ukrainian President Yanukovych tried to hang on to power by adopting a set of anti-protest amendments. The legal acts took an approach similar to that of the Russian legislators, particularly in their interpretation of the term 'extremism'. For example, Law 3879 criminalised the dissemination of 'extremist information' and slander, including online, making it punishable by fines or in some cases by imprisonment.[552] However, those legislative acts were annulled when a new Ukrainian government came into power in 2014.

---

[548] Pollicino and Soldatov, 'Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (n 454).

[549] 'Freedom on the Net 2017: Russia' (*Freedom House*) <https://freedomhouse.org/report/freedom-net/2017/russia> accessed 14 September 2019.

[550] In 2014, Russia held an unlawful referendum in Crimea − part of Ukrainian territory − and subsequently annexed the peninsula. See under Section 3.2.4, *'Ukraine: Crimea and Donbas'*.

[551] 'Russian Efforts At Internet Censorship' (n 547); Kravchenko (n 534).

[552] 'Yanukovych Commits Ukraine to Authoritarian Path' (*RSF*, 20 January 2014) <https://rsf.org/en/news/yanukovych-commits-ukraine-authoritarian-path> accessed 23 June 2019.

The Council of Ministers of Belarus in August 2014 adopted Ruling No. 810,[553] which established a National Expert Committee to Assess Information Products for Containing Extremist Materials. This body was made accountable to the Ministry of Information with a mandate to evaluate the content for the purpose of searching for signs of extremism. The committee was empowered, *inter alia*, to request specific materials for examination. State bodies, businesspersons, and CSOs could be requested to present material for examination.[554]

The amendments to the Belarusian Media Law of December 2014 significantly extended the authority of the state to block unwanted online outlets. The provisions of Article 38, which forbids the 'propagation of war, violence, cruelty, extremist activities or containing calls for such activities, and also other information' was amended with a vague restriction – the *'dissemination of information which can harm the national interests of the Republic of Belarus'.*[555] As soon as the amendments came into force, the government blocked the independent news outlet Charter 97 and online stores for streaming 'currency panic'.[556] In 2018, Charter 97 was blocked under the same article for spreading banned 'extremist' content and other information that was considered harmful to Belarusian interests.[557]

---

[553] Resolution of the Council of Ministers of the Republic of Belarus 'On expert commissions for evaluating information products for the presence (absence) of signs of extremism' 2014 [810].

[554] 'Mass Media Week in Belarus' <https://baj.by/sites/default/files/analytics/files/11-24_08_2014en.pdf> accessed 14 September 2019; 'Mass Media in Belarus: E-Newstseller' (n 535).

[555] Andrei Bastunets, 'Analysis of Amendments to Media Law' (*BAJ*, 22 January 2015) <http://old.baj.by/be/node/27559> accessed 22 June 2019.

[556] 'Belarus Adopts Restrictive Media Law Amendments, Blocks Websites' (*Committee to Protect Journalists*, 23 December 2014) <https://cpj.org/2014/12/belarus-adopts-restrictive-media-law-amendments-bl.php> accessed 14 September 2019. Russian currency lost its value under the Western sanctions, which affected Belarusian currency. See Agence France Presse, 'Belarus Blocks Online Sites and Closes Shops to Stem Currency Panic' *The Guardian* (21 December 2014) <https://www.theguardian.com/world/2014/dec/21/belarus-blocks-online-websites-shops-currency-panic-rouble> accessed 14 September 2019.

[557] 'Blocking of Leading Belarusian News Website Seen as Test for EU' (n 534).

In the Central Asia region, the reasons behind reinforcing anti-extremism legislation seemed to have different roots, including, in particular, an ethnic and religious basis.[558] However, even though the combating of terrorism might appear to be a legitimate measure in Central Asia, the situation often continues to be used as an excuse for governments to target any critical expression. The laws completely failed to meet international requirements to ensure freedom of expression, assembly, and religion. Undoubtedly, the states here were and are facing a growing threat from radical Islamist organisations such as ISIS, Hizb ut-Tahrir, and IMU.[559] The republics of Kazakhstan, Uzbekistan, and Kyrgyzstan have become targets not only for recruiting members of fundamentalist organisations but also of terrorist attacks.[560] Russia encountered a similar threat of jihadism spreading through the North Caucasus region,[561] which had lived through a shift from fighting for the independence of the Chechen Republic to the cause of espousing radical Islam.[562]

The Kyrgyz and Kazakh governments modelled their legislative framework for countering terrorism in accordance with the Russian 'Law on Countering Extremist Activities'.[563] As a result, the countries followed suit to replicate similar practices, and any public expression involving issues that the authorities considered sensitive could lead to

[558] Pollicino and Soldatov, 'Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (n 454).
[559] Anna Matveeva, 'Radicalisation and Violent Extremism in Kyrgyzstan: On the Way to the Caliphate?' (2018) 163 The RUSI Journal 30.
[560] ibid; Shirin Akiner, *Kyrgyzstan 2010: Conflict and Context* (Central Asia-Caucasus Institute 2016).
[561] Svante Cornell and Michael Jonsson, *Conflict, Crime, and the State in Postcommunist Eurasia* (University of Pennsylvania Press 2014) 82–102.
[562] Pollicino and Soldatov, 'Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (n 454) 96–97.
[563] Inga Sikorskaya, 'V Kyrgyzstane smeshany ponyatiya razzhiganiya rozni i ekstremizma. K chemu eto privodit? [The concepts of inciting hatred and extremism are mixed in Kyrgyzstan. What does this lead to?]' (*Kaktus.media*, 8 October 2018) <https://kaktus.media/doc/379652_v_kyrgyzstane_smeshany_poniatiia_razjiganiia_rozni_i_ekstremizma._k_chemy_eto_privodit.html> accessed 14 September 2019.

accusations of extremism.[564] Owing to vague and ambiguous formulations in the laws, any critical media article or report could be qualified as forbidden material. The current data show a similar leaning towards an overwhelming misuse of anti-extremism interpretations in Russia, Kyrgyzstan, and Kazakhstan over the last few decades. In particular, human rights organisations have expressed their grave concern with respect to:

- Article 299-2 of Kyrgyzstan's Criminal Code. The amendments of 2013 criminalised the possession of extremist material even if the accused person had no intention of disseminating the material.[565] The Human Rights Watch reported that at least 258 people were convicted during 2010-2018 with respect to this vaguely defined article, and the number of new cases was increasing each year.[566] Public pressure called for the article to be revised, and, as a result, in 2019 the provision regarding the objective of spreading extremist material was returned to the new Criminal Code.[567]

- Article 174 of Kazakhstan's Criminal Code. The provision was criticised by local human rights defenders, by the UN Special Rapporteur on the right to freedom of peaceful assembly and of association, and by the Human Rights Committee for the

[564] Begaim Usenova, 'V KR po stat'ye 299 cheloveka mogut posadit' za vpolne bezobidnyye frazy [In the Kyrgyz Republic, under Article 299, people can be imprisoned for uttering completely harmless phrases]' (*Radio Azattyk*, 3 May 2018) <https://rus.azattyk.org/a/kyrguzstan-usenova-law/29206193.html> accessed 14 September 2019; Bruce Pannier, 'The Victims Of Kazakhstan's Article 174' (*RadioFreeEurope/RadioLiberty*, 2 February 2016) <https://www.rferl.org/a/qishloq-ovozi-kazakhstan-article-174/27527738.html> accessed 14 September 2019.

[565] Criminal Code of Kyrgyz Republic 1997 [68]; 'Zashchitit Li Konstitutsiya Kyrgyzskoy Respubliki Veruyushchikh Ot Ugolovnogo Presledovaniya Za Deystviya, Ne Predstavlyayushchiye Obshchestvennoy Opasnosti [Will the Constitution of the Kyrgyz Republic Protect Believers from Criminal Prosecution for Actions That Do Not Pose a Public Danger?]' (*Koom.kg*, 2017) <http://www.koom.kg/index.php?act=material&id=3762> accessed 14 September 2019.

[566] '"We Live in Constant Fear": Possession of Extremist Material in Kyrgyzstan' (*Human Rights Watch*, 17 September 2018) <https://www.hrw.org/report/2018/09/17/we-live-constant-fear/possession-extremist-material-kyrgyzstan> accessed 25 June 2019.

[567] Criminal Code of the Kyrgyz Republic 2017 [19].

lack of a clear definition of the terms 'incitement of discord',[568] 'extremism', 'inciting social or class hatred', and 'religious hatred or enmity'.[569] Since 2015, the number of citizens accused under this article has increased by up to 20 cases.[570]

- Article 282 of the Russian Criminal Code. This article criminalised the incitement of hatred or the debasement of human dignity based on group characteristics.[571] The media referred to this provision as a 'Meme Law', given that many social media users were convicted under this article for posting pictures on sensitive topics online.[572] The SOVA Center reports a gradual increase in the number of cases of what is termed an extremist nature from 2010 to mid-2017[573] but a subsequent decline in the trend. In 2019, Article 282 was partly decriminalised;[574] however, the 'general repressive quality' of anti-extremism legislation left few grounds for enthusiasm.[575]

---

[568] Kiai M, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai: Mission to Kazakhstan 2015 [A/HRC/29/25/Add.2].

[569] Human Rights Committee, Concluding observations on the second periodic report of Kazakhstan 2016 [CCPR/C/KAZ/CO/2].

[570] Felix Corley, 'Kazakhstan: Article 174 Cases Increase, Cancer Sufferer Tortured' (Forum 18 2017) <https://www.refworld.org/docid/58bfbe4c4.html> accessed 14 September 2019; Pannier (n 564).

[571] In the Criminal Code of Russian Federation 1996 [63-FZ] Art. 282.2., violation is defined as follows: 'Actions aimed at inciting hatred or enmity, as well as at humiliating the dignity of a person or group of people on the grounds of sex, race, nationality, language, origin, religion, as well as belonging to any social group, committed publicly, including using the media or information and telecommunication networks, particularly the Internet'. The violation is punishable by fines for up to RUB 600 000 (€8 500) or imprisonment for up to six years.

[572] Evan Gershkovich, 'Will Russia Stop Arresting Its Citizens For Posting Memes?' (*The Moscow Times*, 4 October 2018) <https://www.themoscowtimes.com/2018/10/04/will-russia-stop-arresting-citizens-for-memes-a63090> accessed 14 September 2019; Lyubov Chizhova, Yelizaveta Mayetnaya and Robert Coalson, 'Only A Few "Likes" For Putin's Softening Of Controversial Meme Law' (*Radio Free Europe/Radio Liberty*, 2018) <https://www.rferl.org/a/russia-putin-meme-laws-softening-critics-stifling-dissent-freedom-speech/29527682.html> accessed 14 September 2019; Andrew Roth, 'Young Russians Posting Memes Face Jail for "Extremism"' *The Guardian* (1 September 2018) <https://www.theguardian.com/world/2018/sep/01/young-russians-posting-memes-face-jail-for-extremism> accessed 14 September 2019.

[573] Alexander Verkhovsky, 'A New Turn of the Kremlin's Anti-Extremist Policy' (*SOVA Center*, 2019) <http://www.sova-center.ru/en/misuse/reports-analyses/2019/04/d40960> accessed 14 September 2019.

[574] Gershkovich (n 572); Chizhova, Mayetnaya and Coalson (n 572).

[575] Verkhovsky (n 573).

During 2013, prior to the post-Euromaidan legislative amendments in Russia and Belarus, the Republics in Central Asia demonstrated a move towards harshening anti-extremist laws.

In January 2013, the Kazakh government adopted new amendments to the law to counter terrorism. The new legal provisions broadened the jurisdiction of security services and iterated an unclear formulation of the phrase 'fomenting social discord'.[576] According to the amendments, the mass media should be willing to cooperate with anti-terrorist security bodies, although the mechanism remains unclear.[577]

In February 2013, Kyrgyzstan's Law on Counteracting Extremist Activities was revised. As a consequence, the government was enabled to block foreign websites on Kyrgyz territory in the event of 'extremist' content being detected.[578] In this way, the government made an effort to deal with the domestic situation as well as with tensions following on from the clashes between Kyrgyz and the Uzbek minorities in June 2010.[579]

Georgia is another example of a country that has had to revise its legislation owing to a growing threat of radical Islamism. The US Department of State reported that considering Georgia's geographic position, 'Islamist extremists have transited through the country between the Russian Federation's North Caucasus, Iraq, Syria, and Turkey'.[580] Therefore, in June 2015, Georgia amended its anti-terrorist legislation to criminalise foreign fighters and

[576] Law of the Republic of Kazakhstan 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Counter-Terrorism Issues' 2013 [63–V].
[577] 'Freedom on the Net 2014: Kazakhstan' (*Freedom House*, 26 November 2014) <https://freedomhouse.org/report/freedom-net/2014/kazakhstan> accessed 14 September 2019.
[578] 'Vo Vtorom Chtenii Prinyaty Popravki v Zakon o Protivodeystvii Ekstremistskoy Deyatel'nosti [The Second Reading Adopted Amendments to the Law on Countering Extremist Activities]' (*For.kg*, 2013) <https://www.for.kg/news-216159-ru.html> accessed 14 September 2019.
[579] Anna Matveeva, Igor Savin and Bahrom Faizullaev, 'Kyrgyzstan: Tragedy in the South' (2012) 17 Ethnopolitics Papers.
[580] 'Country Reports on Terrorism 2016: Georgia' (United States Department of State 2017) <https://www.refworld.org/docid/5981e43ea.html> accessed 14 September 2019.

participation in international terrorism.[581] Largely, the document was prepared in line with UN Security Council Resolution 2178.[582] The new provisions were formulated sufficiently clearly, but human rights activists were concerned that amendments would be applied selectively to suppress online expression.[583]

The second 'wave' of anti-terrorist measures began in 2016, and was broadly associated with the 'Yarovaya Law' in Russia, which was adopted in July 2016.[584] The legal novelties may be divided into several broad categories, and manifest the significant empowering of security bodies to gain access to personal communication through tougher requirements for mobile and Internet operators. The measures have to do with the storage of personal information and the new requirements with regard to delivery and postal services. The provisions to ensure greater state control over online communication, such as an obligation to uncover encrypted communication, elicited a particularly vocal response from the public. Because the text of the Yarovaya Law includes a long list of stifling measures, frequent references to relevant items will be made throughout this section.

In April 2016, the Uzbekistan government introduced amendments to Article 244 of the Criminal Code. The changes concerned the media and Internet limitations, and allowed authorities to re-categorise extremism from being an administrative to a criminal offence, even if committed for the first time.[585] Commenting on these changes, the OSCE Representative on Freedom of the Media stressed that 'Anti-terror legislation should not use

---

[581] Law of Georgia 'On Amendments to the Criminal Code of Georgia' 2015 [3699-II c].
[582] UN Security Council, Resolution 2178 (2014) Adopted by the Security Council at its 7272nd meeting 2014 [S/RES/2178].
[583] 'Freedom on the Net 2016: Georgia' (*Freedom House*, 9 November 2016) <https://freedomhouse.org/report/freedom-net/2016/georgia> accessed 22 June 2019.
[584] Maria Kravchenko, 'Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2016' (*SOVA Center*, 2017) <http://www.sova-center.ru/en/misuse/reports-analyses/2017/04/d36857> accessed 14 September 2019.
[585] Mushfig Bayram, 'UZBEKISTAN: Harshened Criminal and Administrative Code Punishments' (*Forum 18*, 15 June 2016) <http://www.forum18.org/archive.php?article_id=2189> accessed 14 September 2019.

overly broad definitions to preclude a journalist from working on problematic issues of public interest'.[586]

In the period 2016-2017, the Kyrgyz government also focused on the development of counter-terrorism legislation. The fact of radicalisation of the Central Asia region had to be recognised internationally when four terrorist attacks within just one year − in New York, St Petersburg, Istanbul, and Stockholm − were carried out by individuals of Uzbek origin.[587] In addition, a range of local incidents of a terrorist nature occurred: for example, the bombing of the Chinese Embassy in Bishkek. To bring the situation under control, in 2016 the Kyrgyz president signed a set of legal amendments that allowed the state to strip Uzbek citizenship from those who participated in terrorist attacks abroad or who receive terrorism-related training.[588] New provisions banning public expressions of approval and justification of extremism or terrorism online were added to the criminal code.[589] That being said, the recent practice saw an increasing number of cases where the government blocked independent news sites on the grounds of combating extremism. For instance, the leading news agency, Ferghana.News, was blocked in 2017, and the step was defined by international journalist organisations as 'an act of censorship unworthy of Kyrgyzstan's democracy'.[590] This was not the first time this outlet had been targeted.[591] In 2017, the authorities blocked Archive.org, a website that enables access to deleted web pages. Users suggested that it was not 'extremist'

[586] 'Recent Legislative Amendments in Uzbekistan Worrying, OSCE Representative Says' (*OSCE*, 29 April 2016) <https://www.osce.org/fom/237641> accessed 14 September 2019.
[587] Matveeva (n 559).
[588] 'Country Reports on Terrorism 2016: Kyrgyz Republic' (United States Department of State 2017) <https://www.refworld.org/docid/5981e43013.html> accessed 14 September 2019.
[589] ibid.
[590] 'Kyrgyzstan Censors Leading News Agency Ferghana' (*IFEX*, 14 June 2017) <https://ifex.org/kyrgyzstan-censors-leading-news-agency-ferghana/> accessed 25 June 2019.
[591] See, for instance, 'Independent News Website Partly Blocked In Kyrgyzstan' (*RadioFreeEurope/RadioLiberty*, 22 February 2012) <https://www.rferl.org/a/independent_news_website_partly_blocked_in_kyrgyzstan/24492408.html> accessed 25 June 2019.

content that prompted the government's action but rather the availability of articles criticising the government.[592]

New anti-extremist legal provisions were also adopted in Kazakhstan. According to the amendments of March 2017, the courts were authorised to deprive Kazakh individuals of their citizenship if 'they harm the vital interests' of Kazakhstan.[593] In a move almost mirroring the Russian legislative framework, President Nazarbayev in December 2016 signed amendments that granted more power to law enforcement bodies and limited the use of encrypted communication.[594] In August 2017, Kazakh authorities reported the blocking of 30,000 websites in the course of that year. The blocked pages featured a medley of topics, including pornography, extremism, terrorism, and calls for violence.[595] There was ample evidence that activists, independent journalists, and ordinary citizens sharing opposing views were increasingly targeted on the grounds of anti-terrorism.[596] For instance, Almat Zhumagulov and Kenzhebek Abishev, members of the WhatsApp group discussing political issues, were accused of propagating terrorism.[597] Their lawyers believed the charges were politically motivated and related to their dissenting activities.

In the aftermath of the annexation of Crimea in 2014 and the armed conflict that followed in Eastern Ukraine, the Ukrainian government resorted to anti-terrorism legislation

---

[592] Akhal-Tech Collective, 'Kyrgyzstan Blocks Archive.Org on "Extremism" Grounds' (*Global Voices*, 21 July 2017) <https://globalvoices.org/2017/07/21/kyrgyzstan-blocks-archive-org-on-extremism-grounds/> accessed 22 June 2019.

[593] Aigerim Toleukhanova, 'Kazakhstan: Parliament Rams Through Vague Constitution Fix' (*Eurasianet*, 6 March 2017) <https://eurasianet.org/kazakhstan-parliament-rams-through-vague-constitution-fix> accessed 14 September 2019.

[594] 'Country Reports on Terrorism 2016: Kazakhstan' (United States Department of State 2017) <https://www.state.gov/reports/country-reports-on-terrorism-2016/> accessed 14 September 2019.

[595] 'Boleye 30 tys. saytov za god blokiruyetsya v Kazakhstane [More than 30 thousand sites during that year are blocked in Kazakhstan]' (*Digital Report*, 8 June 2017) 30 <https://digital.report/bolee-30-tyis-saytov-za-god-blokiruetsya-v-kazahstane/> accessed 14 September 2019.

[596] 'Kazakhstan: Strikes, Arrests and Fears of New Restrictions on Fundamental Freedoms' (*CIVICUS*, 31 January 2018) <https://monitor.civicus.org/newsfeed/2018/01/31/kazakhstan-strikes-arrests-and-fears-new-restrictions-fundamental-freedoms/> accessed 25 June 2019.

[597] Joanna Lillis, 'Kazakhstan: Terrorist Plot — or Concocted Conspiracy?' (*Eurasianet*, 2 February 2018) <https://eurasianet.org/kazakhstan-terrorist-plot-or-concocted-conspiracy> accessed 25 June 2019.

to target pro-Russian separatist groups. According to Freedom House reports, a number of criminal charges were made against social media users who 'call for extremism and separatism'.[598] However, the overall statistics remain inaccurate. The Security Service of Ukraine (SBU) announced 60 convictions from 2015 to 2017,[599] whereas the other report suggested there were 37 convictions in 2017 alone for anti-Ukrainian content in social media groups.[600] It should be noted, that Ukrainian legislation has not, to date, developed a law specifically covering ICTs. However, general criminal violations have been extended to online activities, and individuals have been sentenced under Articles 109, 110 of the Criminal Code. Violation of Article 109, *'Actions aimed at forcibly altering or overthrowing the constitutional order or seizing state power',* is punishable for up to 10 years of imprisonment. Violation of Article 110, *'Infringement upon the territorial integrity and inviolability of Ukraine'*, is punishable by up to five years of imprisonment. Neither article provides for punishment other than imprisonment, such as fines, public works, or some other form.[601]

The emergence of the self-proclaimed republics in Eastern Ukraine disturbed the international community, including Kazakhstan, which has high numbers of ethnic Russians in the northern regions of the country. The concerns are not groundless, as over the last few years several citizens have been charged with criticising the Russian occupation of Kazakhstan.[602]

---

[598] 'Freedom on the Net 2018: Ukraine' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/ukraine> accessed 14 September 2019.
[599] '72 criminal proceedings of "anti-Ukraine" propaganda cases registered in 2015-2017' (*Net Freedom*, 23 October 2017) <https://netfreedom.org.ua/72-criminal-proceedings-of-anti-ukraine-propaganda-cases-registered-in-2015-2017/> accessed 14 September 2019.
[600] *See* 'Ponad 30 vlasnykiv ta administratoriv antyukrayins′kykh spil′not u sotsmerezhakh otrymaly vyroky sudu - SBU [More than 30 owners and administrators of anti-Ukrainian communities in social networks received verdicts of the court - the SBU]' (*detector.media*, 28 October 2017) <https://detector.media/infospace/article/131371/2017-10-28-ponad-30-vlasnikiv-ta-administratoriv-antiukrainskikh-spilnot-u-sotsmerezhakh-otrimali-viroki-sudu-sbu/> accessed 14 September 2019.
[601] Criminal Code of Ukraine 2001 [2341–III].
[602] Pannier (n 564).

The mentioned cases involving Russia, Belarus, and Central Asian states are distinctive from other sub-regional groups. The major peculiarity is that the former examples pose 'extremism' as a criminal offence (as described above in this section), whereas the Criminal Codes of Ukraine,[603] Georgia,[604] Estonia,[605] Armenia,[606] contain provisions only regarding 'terrorism'.

Overall, the reasons behind the process of toughening anti-terrorism legislation differ across the post-Soviet states. Nonetheless, there is a discernible pattern in re-working the legislative frameworks within the region. The trend is for legal texts to provide vague definitions of the key terms, and to grant the state a wide-ranging power that can stifle freedom of expression. There is a growing body of evidence that state initiatives and measures designed to combat extremism are implemented aggressively and indiscriminately throughout the Russian Federation and Central Asia.

Drawing from the approaches of benchmark countries under *Section 5*, and taking into account the recommendations of international organisations with respect to counter-terrorism approaches in the post-Soviet region, the author suggests that the following may be undertaken to eliminate common legislative deficiencies within the analysed region:

- ensure clear and precise wording of key definitions on national security;[607]
- ensure legality, legitimacy, and proportionality of restrictions with respect to other human rights, particularly the right to freedom of expression.[608]

---

[603] Criminal Code of Ukraine (n 601) Art 258, 258.1, 258.2, 258.3, 258.4, 258.5.
[604] Criminal Code of Georgia 1999 ch XXXVIII.
[605] Penal Code of Estonia 2001 [RT I, 19.03.2019, 3] Art. 237, 237.1, 237.2, 237.3.
[606] Criminal Code of the Republic of Armenia 2003 [ZR-528] Art. 217.
[607] As suggested, for instance, in 'Misuse of Anti-Terror Legislation Threatens Freedom of Expression' (n 531); 'Joint Declaration on Media Independence and Diversity in the Digital Age' (n 532). Also, in legal analysis of particular state practices: Venice Commission Opinion on the Federal Law on Combating Extremist Activity of the Russian Federation (n 538); Human Rights Committee Concluding observations on the second periodic report of Kazakhstan (n 569).

6.1.2. Criminal Defamation Laws

The overall picture of how defamation-related measures are applied in the region is unclear. On the one hand, several countries in post-Soviet territory have implemented progressive reforms and abolished criminal defamation and insult laws.[609] On the other hand, a number of countries have resorted to measures that have strengthened the provisions on defamation. The latter countries comprise the Russian Federation, Belarus, Azerbaijan, and the countries of Central Asia – Uzbekistan and Kazakhstan. These countries established general criminal legislation on defamation, as well as special laws on insulting authorities and state leaders. Defamation-related violations in these jurisdictions provide for the most stringent sanctions, including a prison sentence. Moreover, the states have introduced legislation that specifically addresses online speech. A variety of charges are commonly applied to prevent the circulation of critical views regarding government officials and institutions.

In July 2012, an article on slander was returned to the criminal code of the Russian Federation.[610] Violation of this article is punishable by fines and community service. Additionally, the code included articles regarding insulting a representative of state authority (Art. 319), contempt of court (Art. 297), and slander against prosecutors, judges, and investigators (Art. 298.1).[611] The first two provisions were introduced back in 1996, in the initial Criminal Code, whereas Article 298.1 was adopted in July 2012.[612]

---

[608] UN Human Rights Committee General comment No. 34. Article 19: Freedoms of opinion and expression (n 387); 'Joint Declaration on Media Independence and Diversity in the Digital Age' (n 532).
[609] For instance, defamation was decriminalised in Ukraine (2001), Estonia (2002), Georgia (2004), Moldova (2004, partially), and Armenia (2010).
[610] Federal law 'On Amendments to the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation' 2012 [141-FZ].
[611] Scott Griffen, 'Defamation and Insult Laws in the OSCE Region: A Comparative Study' [2017] Vienna: Organization for Security and Co-operation in Europe 195–197.
[612] Criminal Code of Russian Federation (n 571) Art. 298.1.

As early as 2004, Internet operators in Uzbekistan were prohibited from disseminating information 'containing…infringements upon the honour and dignity of a person'.[613] The current Criminal Code of the Republic of Uzbekistan,[614] the Administrative Liability Code of the Republic of Uzbekistan,[615] contains provisions with respect to defamation and insults. The 'Law on the Status of the Deputy of the Legislative Chamber and Member of the Senate of the Oliy Majlis of the Republic of Uzbekistan' provides for the inviolability of deputies' honour and dignity.[616] Article 284 of the Criminal Code establishes liability for an 'insult by a subordinate of his superior and insult by a superior of his subordinate', with a maximum penalty of one year of imprisonment. The 'Law on the Fundamental Guarantees for the Activities of the President of the Republic of Uzbekistan' guarantees protection of the president's honour and dignity.[617]

In 2010, the 'Law on the Leader of the Nation' was passed in Kazakhstan. This status granted President Nazarbayev the authority to take state-related decisions even after his term of office had expired, and provided immunity with regard to any action he had taken while in presidential office. Public insults or other encroachments on the honour and dignity of the First President of the Republic of Kazakhstan are prosecuted.[618]

Article 130 and 131 of the Kazakhstan Criminal Code criminalises public defamation and insult.[619] According to the media, the Kazakhstan courts heard the first case of online

[613] Order of the Uzbek Agency of Communication and Informatization 'On the Approval of the Provision of Access to the Internet in Public Areas' 2004 [216].
[614] Art. 139, 140.
[615] Art. 40, 41.
[616] The Law 'On the Status of the Deputy of the Legislative Chamber and Member of the Senate of the Oliy Majlis of the Republic of Uzbekistan' 2004 [704–II] Art. 12.
[617] The Law 'On the Fundamental Guarantees for the Activities of the President of the Republic of Uzbekistan' 2003 [480–II] Art. 4.
[618] INFORM.KZ (n 33).
[619] Criminal Code of the Republic of Kazakhstan 2014 [226–V].

libel in 2013.[620] Two officers of the Almaty Tax Department were prosecuted for publishing an anonymous message in the Tax Committee Chairman's blog, accusing their supervisors of corruption.

Furthermore, Kazakhstan' Criminal Code contains provisions on criminal responsibility for insulting MPs, public officers, judges, prosecutors, and the head of state.[621]

In May 2013, the Azerbaijani government adopted legal amendments on online defamation. According to the new provisions of the criminal code, online defamation is punishable by imprisonment for a maximum of six months. The length of administrative detentions was increased from 15 days to 3 months. Moreover, the Prosecutor and the Ministry of the Interior are authorised to launch an investigation on the basis of Facebook publications.[622]

In January 2014, changes to Articles 9.2 (Libel) and 9.3 (Insult) of the Belarus Code of Administrative Offences annulled the minimum penalty rates for defamatory crimes.[623] On the criminal side, amendments to the criminal code in Belarus took effect in January 2015.[624] The modifications made it a criminal offence to distribute online any content deemed defamatory and a threat to national security.[625] Individuals charged with libel with respect to the head of state ,[626] or with insulting judges[627] and public agents,[628] are also subject to

---

[620] Asem Sakenova, 'Kleveta v Internete [Internet Slander: Almaly Court Examined the First Case of Insult on the Internet]' (*Nomad*, 30 January 2013) <http://nomad.su/?a=13-201301300007> accessed 19 June 2019.
[621] Griffen (n 611) 129–131.
[622] 'Freedom on the Net 2016: Azerbaijan' (*Freedom House*, 10 November 2016) <https://freedomhouse.org/report/freedom-net/2016/azerbaijan> accessed 19 June 2019.
[623] The Law of the Republic of Belarus 'On introducing amendments and addenda to the Code of the Republic of Belarus on Administrative Offenses and the Procedure Executive Code of the Republic of Belarus on Administrative Offenses' 2014 [120-Z]; Griffen (n 611) 55.
[624] Art. 188, 361, and 367.
[625] The Law of the Republic of Belarus 'On introducing amendments to the Criminal, Criminal Procedure, Criminal Executive Codes of the Republic of Belarus, the Code of the Republic of Belarus on Administrative Offenses and the Procedural Executive Code of the Republic of Belarus on Administrative Offenses' 2015 [241-Z].
[626] Criminal Code of the Republic of Belarus 1999 [275-3] Art. 367, 368.
[627] ibid Art. 391.

criminal sanctions. Earlier in 2006, Article 19 stressed that criminal defamation laws are applied broadly in Belarus, specifically with respect to protection of the president.[629]

Although Estonian legislation of does not contain general defamation laws, there are several clauses regarding defamation of public officials in the Criminal Code. Article 275, which entered into force on January 2015, makes it a criminal offence to 'insult […] a representative of state authority protecting public order in connection with performance of his or her official duties'. The violation is punishable by a fine of 1200 euro or detention, and 3200 euro for legal persons. 'Defamation of a representative of state authority in connection with performance of his or her official duties', according to Article 275.1, may lead to a maximum two-year prison term.

In November 2016, Azerbaijan authorities introduced new provisions and increased penalties for online insults and libel. According to Article 148-1 of the Criminal Code, insults and slander under fake user-names, profiles, and accounts became punishable by a maximum of AZN 1 500 (€800),[630] 480 hours of community labour, two years of corrective work, or one year of imprisonment.[631] In addition, an amendment to Article 323 imposed penalties of up to AZN 1 500 (€800)[632] and a three-year prison term for insulting the honour and dignity of the president via fake accounts.[633] The amended Criminal Code increased a prison term by up to three years for libel (Article 147-2). According to Article 147-1, dissemination, in a public statement, publicly exhibited work of art, through the mass media or a publicly displayed Internet information resource, of knowingly false information discrediting the honour and dignity of a person or damaging his or her reputation is punishable by a

---

[628] ibid Art. 369.
[629] 'Defamation Law and Practice in Belarus, Moldova and Ukraine' (Article 19 2006) 3–4.
[630] In the last version of the article, the penalty has been increased to AZN 2 000 (€1 070).
[631] U. S. Department of State, '2016 Country Reports on Human Rights Practices - Azerbaijan' (U S Department of State 2017) <https://www.refworld.org/docid/58ec8a753.html> accessed 19 June 2019.
[632] Currently punishable by a 3-year term of imprisonment.
[633] U. S. Department of State (n 631); Griffen (n 611) 49.

maximum prison sentence of six months. Under Article 289, it is a criminal offence to show disrespect to a court and to insult judges and participants at a hearing.[634]

A notable legal case was under scrutiny in Armenia in March 2017. According to the court decision, the YouTube channel SOS TV, after publishing a satirical video on Armenian police, was obliged to apologise for damaging the honour and dignity of the law enforcement officers.[635] It must be noted that the Armenian legislation had contained no general criminal provisions regarding defamation since May 2010.[636] Issues with respect to insults and libel are handled within civil law jurisdiction. Nonetheless, the Criminal Code incorporates provisions regarding the defamation of judicial and investigative authorities.[637]

The Azerbaijan Criminal Code was modified in May 2017. Amendments to Article 323(1) announced imprisonment for up to five years for defamation and for insulting the honour and dignity of the president, particularly in statements and posts on social media platforms.[638]

In Kyrgyzstan, defamation and insult are not subjects of criminal liability. Instead, the clauses regarding personal reputation are included to the Civil Code.[639] As to the defamation of state officials, the *Law 'On guarantees of the activities of the President of the Kyrgyz Republic and the status of the ex-president of the Kyrgyz Republic'* rules that the

[634] Griffen (n 611) 48–49.
[635] Ruzan Gishyan, 'Datarany Masnakioren Bavararets' Vostikanut'yan Hayts'n Ynddem SOS TV-i [The Court Partially Satisfied the Lawsuit Filed by the Police against SOS TV]' (*Radio Free Europe/Radio Liberty Armenian Service*, 14 March 2017) <https://www.azatutyun.am/a/28368592.html> accessed 19 June 2019.
[636] Griffen (n 611) 42.
[637] Art. 344
[638] 'Freedom on the Net 2017: Azerbaijan' (*Freedom House*, 14 November 2017) <https://freedomhouse.org/report/freedom-net/2017/azerbaijan> accessed 19 June 2019.
[639] Civil Code of Kyrgyz Republic 1996 [15] Part I, Art 18.

dissemination of information harming the honour and dignity of the president may require compensation for the moral damage.[640]

In March 2017, the General Prosecutor of Kyrgyzstan filed a series of lawsuits targeting the independent media outlets Zanoza.kg and Radio Azattyk (Radio Free Europe/Radio Liberty local service). The media were charged with defamation of the honour and dignity of the president.[641] In August 2017, the Bishkek Court rejected appeals by Zanoza, and ordered the media outlet to pay KGS 12 million (€157 000) in moral compensation.[642] A number of civil rights organisations expressed their concern with respect to the case, and stressed that the court decisions were politically motivated and unwarranted.[643]

All things considered, it is difficult to draw clear a distinction between sub-regional groups with regard to defamation laws. A notable pattern is represented by the Russian Federation, Belarus, Azerbaijan, Kazakhstan, and Uzbekistan, which establish general criminal defamation provisions, but also involving defamation against public officials and the head of state. In the meantime, whereas several post-Soviet countries bloc have decriminalised defamation in recent years, the clauses regarding the defamation of public officials remain – in a certain form – in the legislative frameworks, as shown by the examples of Estonia and Armenia. Moreover, even when defamation is a subject of civil liability, it

---

[640] The Law 'On guarantees of the activities of the President of the Kyrgyz Republic and the status of the ex-president of the Kyrgyz Republic 2003 [152] Art 4.

[641] 'Kyrgyzstan: Growing Pressure on Media Groups' (*Human Rights Watch*, 27 March 2017) <https://www.hrw.org/news/2017/03/27/kyrgyzstan-growing-pressure-media-groups> accessed 19 June 2019.

[642] 'Kyrgyzstan: Stop Legislative Harassment of Zanoza.Kg and Its Journalists' (*ARTICLE 19*, 12 August 2017) <https://www.article19.org/resources/kyrgyzstan-stop-legislative-harassment-of-zanoza-kg-and-its-journalists/> accessed 19 June 2019.

[643] 'Kyrgyzstan: Growing Pressure on Media Groups' (n 641); 'Kyrgyzstan: Stop Legislative Harassment of Zanoza.Kg and Its Journalists' (n 642); 'Kyrgyzstan Holds Three Trials in One Day against Independent Outlet' (*Committee to Protect Journalists*, 29 June 2019) <https://cpj.org/2017/06/kyrgyzstan-holds-three-trials-in-one-day-against-i.php> accessed 19 June 2019; 'Kyrgyzstan: Human Rights Defenders, Independent Media Targeted in Defamation Case' (*Freedom House*, 2 May 2017) <https://freedomhouse.org/article/kyrgyzstan-human-rights-defenders-independent-media-targeted-defamation-case> accessed 19 June 2019.

may be used as an excuse to oppress free expression, as was exemplified with regard to independent media outlets in Kyrgyzstan.

As to recommendations for the countries under scrutiny, the author suggests that lawmakers should remove defamation from the scope of criminal violations, especially when dealing with the defamation of authorities. Many international organisations have called upon the states to avoid criminal defamation practices, as they may have a chilling impact on freedom of expression and media reporting. The UN Human Rights Committee, for instance, recommended that states decriminalise defamation, noting that 'the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty'.[644] In the *Joint Declaration on Media Independence and Diversity in the Digital Age*, international organisations established as one of the principles for the states to ensure 'that defamation laws are exclusively civil rather than criminal in nature and do not provide for excessive damages awards'.[645]

6.1.3. Laws on fake news

In the midst of heated public discussions *vis-à-vis* online disinformation, a number of countries worldwide have developed policies to combat the threat of fake news, including France, Germany, and the controversial examples of Singapore and Malaysia.[646] The European Commission issued recommendations to improve legal frameworks, urging the states to avoid any form of censorship as a response to fake news.[647] The disturbing trend uncovered by the present research, however, is that authorities commonly fail to adopt

[644] UN Human Rights Committee General comment No. 34. Article 19: Freedoms of opinion and expression (n 387) para 47.
[645] 'Joint Declaration on Media Independence and Diversity in the Digital Age' (n 532).
[646] Fathin Ungku, 'Factbox: "Fake News" Laws around the World' *Reuters* (2 April 2019) <https://www.reuters.com/article/us-singapore-politics-fakenews-factbox-idUSKCN1RE0XN> accessed 20 June 2019.
[647] 'Final Report of the High Level Expert Group on Fake News and Online Disinformation' (*European Commission*, 12 March 2018) <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation> accessed 20 June 2019.

legislation in accordance with international requirements. In a fashion similar to that regarding anti-extremism and defamatory laws, governments suppress independent speech behind the smoke screen of 'protecting their citizens'. This feeble response was demonstrated by a few states that had modernised the provision on disseminating false information to target online speech specifically.

Since 2014, government officials in Kazakhstan have been required to follow the guidelines on their use of the Internet. The rules oblige employees to avoid spreading content critical of the authorities, false information, and leaks, and not to 'befriend' users publishing such information.[648] 'Disseminating knowingly false information', including online, is punishable under the criminal code.[649] In 2017, the Ministry of the Interior registered 25 criminal offences involving the spreading of misinformation via the Internet.[650]

In March 2018, Kazakhstan authorities launched a criminal investigation into two independent media outlets: Forbes Kazakhstan and Ratel.kz.[651] The websites were accused of 'disseminating knowingly false information', because they had published investigations into the corruption of the former government official, Zeinulla Kakimzhanov.[652] On April 2, police searched the offices of both media outlets, and confiscated documents and computers. About the same time, the Ratel.kz page and affiliated websites were blocked on a separate matter, allegedly for violation of media registration requirements. The preliminary decision

[648] Viktor Burdin, 'Gossluzhashchim RK zapretili kritikovat' vlast' v sotssetyakh [State officials not allowed to criticize the power]' (*Forbes.kz*, 12 January 2015) <https://forbes.kz//process/internet/gosslujaschim_i_byudjetnikam_rk_zapretili_kritikovat_vlast_v_sotssetyah/> accessed 20 June 2019.

[649] Criminal Code of the Republic of Kazakhstan (n 619) Art. 274.

[650] Mirkhat Azhigaliev, 'Skol'ko kazakhstantsev osudili za rasprostraneniye lozhnoy informatsii v Internete [How many Kazakhstanis have been convicted for spreading false information on the Internet]' (*Tengrinews.kz*, 15 January 2018) <https://tengrinews.kz/internet/skolko-kazahstantsev-osudili-rasprostranenie-lojnoy-335392/> accessed 20 June 2019.

[651] 'Kazakhstan: Criminal Probe of Media Outlets' (*Human Rights Watch*, 6 April 2018) <https://www.hrw.org/news/2018/04/06/kazakhstan-criminal-probe-media-outlets> accessed 20 June 2019.

[652] It was not the first case of Kakimzhanov accusing Ratel.kz and Forbes.kz of defamation. In April 2017, Almaty's Medeu district court granted the defamation request by Kakimzhanov, and ordered Ratel.kz and Forbes.kz to pay total damages of KZT 50 200 000 (€118 300). See ibid.

was issued on March 21, whereas on May 28, Almaty's Medeu district court ordered a one-year ban of Ratel.kz and its alternative domain name Balborsyk.kz.[653] The court dispute is currently ongoing. [654] Civil rights organisations have harshly criticised all of the aforementioned cases, and called on the Kazakh government to drop the investigation.[655]

In June 2018, legislation targeting 'fake news' was passed in Belarus.[656] Amendments to the Media Law criminalised the spread of false information and imposed liability on website owners for spreading false news, harming national interests, or disseminating defamatory information.[657] The legislation empowered the government of Belarus to block social media and other websites if they were found to be in violation.

In March 2019, Russian Federation lawmakers passed a controversial 'anti-fake news' package. This kit consisted of two bills that regulated the spread of fake news[658] and that penalised 'lack of respect for the authorities'.[659] The first bill banned the spreading of

[653] 'Kazakhstan Shuts Down Independent News Site' (*RadioFreeEurope/RadioLiberty*, 2018) <https://www.rferl.org/a/kazakhstan-shuts-down-independent-news-site-ratel/29254964.html> accessed 16 September 2019.
[654] Ulyana Salapaeva, 'Smozhet Li Marat Asipov Zanimat'sya Zhurnalistikoy? [Will Marat Asipov Be Able to Work as a Journalist?]' (*Forbes.kz*, 14 August 2019) <https://forbes.kz//process/probing/smojet_li_marat_asipov_zanimatsya_jurnalistkoy_deyatelnostyu/> accessed 16 September 2019.
[655] Harlem Désir, 'Blocking of News Website and Detention of Journalists in Kazakhstan of Grave Concern, Says OSCE Representative on Freedom of the Media' (*OSCE*, 5 April 2018) <https://www.osce.org/representative-on-freedom-of-media/376966> accessed 20 June 2019; 'Kazakhstan Should Drop "False Information" Case against Critical Media Outlets' (*International Press Institute*, 13 April 2018) <https://ipi.media/kazakhstan-should-drop-false-information-case-against-critical-media-outlets/> accessed 20 June 2019; '"False Information" Laws Must Not Be Used to Silence the Media in Kazakhstan' (*IFEX*, 18 May 2018) <https://ifex.org/false-information-laws-must-not-be-used-to-silence-the-media-in-kazakhstan/> accessed 16 September 2019.
[656] 'Belarus Passes Legislation Against "Fake News" Media' (*RadioFreeEurope/RadioLiberty*, 14 June 2018) <https://www.rferl.org/a/belarus-assembly-passes-controversial-fake-news-media-legislation/29291033.html> accessed 20 June 2019.
[657] Law 'On making changes and additions to some laws of the Republic of Belarus' 2018 [128-Z].
[658] Federal Law 'On Amening Article 15.3 of the Federal Law 'On Information, Information Technologies and Protection of Information' 2019 [31-FZ].
[659] Federal Law 'On Amending the Federal Law On Information, Information Technologies and Information Protection 2019 [30-FZ].

> *unreliable socially significant information […] which creates a threat to life and (/or) the health of citizens or property, the threat of mass disturbance of public order and (/or) public safety, or the threat of creating or impairing the proper operation of vital elements of transport or social infrastructure, credit institutions, energy facilities, industry, or communications*.[660]

The second bill addressed information that 'displays obvious disrespect for society, the state, the official state symbols of the Russian Federation, the Constitution of the Russian Federation or the bodies exercising state power in the Russian Federation'.[661] Websites violating the rules are to be blocked, whereas private individuals may be fined up to RUB 400 000 (€5 600) for disseminating false information. Any unlawful content is to be blocked within 24 hours.

The European and International Federation of Journalists has condemned the law of 'fake news' in Russia, and has expressed grave concerns that it would have a chilling effect on freedom of the media.[662]

The Armenian Prime Minister, Nikol Pashinyan, recently drew attention to the problem of fake news. During the Cabinet meeting in April 2019, he stressed that 'if some criminal circles spend millions on manipulating public opinion in social media, in the media, then this is a question of national security,' and called for National Security Service to

---

[660] Oreste Pollicino, 'Fundamental Rights as Bycatch – Russia's Anti-Fake News Legislation' (*Verfassungsblog*, 28 March 2019) <https://verfassungsblog.de/fundamental-rights-as-bycatch-russias-anti-fake-news-legislation/> accessed 17 June 2019.

[661] ibid.

[662] 'Russia: EFJ and IFJ Voice Concerns over New Law on Fake News and Respect for State' (*European Federation of Journalists*, 5 April 2019) <https://europeanjournalists.org/blog/2019/04/05/russia-efj-and-ifj-voice-concerns-over-new-law-on-fake-news-and-respect-for-state/> accessed 20 June 2019.

counter disinformation.[663] However, experts claimed that efforts thus far were extended only to critical commenting on Pashinyan's politics, as the day after announcing the fight against fake news the author of a satirical anti-government Facebook group was arrested.

Anti-fake news efforts have not yet spread widely across the analysed region. However, it may be expected that most of the countries, following the global trend, will adopt respective policies in the near future. As for the above-mentioned cases, it seems that regional peculiarity lies in the fact that governments, by appealing to hot-button issues, extend their control over online expression. The author grounds this conclusion, *inter alia*, on the regional specifics in content regulation and the overall environment of media freedom.

It should be noted that although disinformation is not a new phenomenon, it has definitely taken on a whole new scale with the introduction of information and communication technologies.[664] The setting of standards in the light of this challenge is still evolving on a national and an international level. It is problematic, therefore, to evaluate legal approaches in the analysed regions with respect to the rule of law. However, general recommendations were developed in the *Joint Declaration on ''Fake News'', Disinformation and Propaganda.*[665] In particular, international organisations called for the states to deal with fake news in accordance with the following principles:

- to impose restrictions in the same way as with any limitations to freedom of expression (i.e. provided for by law, serving one of the legitimate interests recognised under international law, and necessary and proportionate to protect that interest);

---

[663] Joshua Kucera, 'Pashinyan Takes on "Fake News"' (*Eurasianet*, 9 April 2019) <https://eurasianet.org/pashinyan-takes-on-fake-news> accessed 27 August 2019.

[664] Jacob Soll, 'The Long and Brutal History of Fake News' (*POLITICO Magazine*, 18 December 2016) <http://politi.co/2FaV5W9> accessed 17 June 2019.

[665] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others, Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda 2017 [FOM.GAL/3/17].

- intermediaries shall not be held liable for third-party content unless they 'specifically intervene in that content' or refuse to remove content under court orders.

In addition, the declaration noted that general prohibitions may fall under vague categories like 'false news' or 'non-objective information', and are 'incompatible with international standards' (i.e. the three-part test mentioned in the paragraph above: legality, legitimacy, and proportionality).

6.2. Procedures and measures as enshrined in legislation and practice: takedown of information

Back in 2000, former United States President Bill Clinton joked about China's attempts to control the Internet. He likened Chinese efforts to 'trying to nail Jello to the wall'. Clinton expressed confidence that in the new century – in spite of censorship attempted by the Chinese government and other authoritarian regimes – 'liberty will be spread by cell phone and cable modem'.[666] Decades later, it is clear that the joke could not have been further from the truth, as numerous countries now control online speech with varying degrees of success. This list includes the states under consideration.

Increasingly restrictive Internet legislation in the post-Soviet countries can be attributed both to global and to local factors. During the early 2000s, a wave of social protest and revolutions took place in many countries; these included the Spanish anti-austerity movement, the Occupy Wall Street movement,[667] and the Arab Spring uprisings. These events confirmed social networks to be powerful tools for revolution. Suddenly, the world found itself in a situation where 'dictatorships could be overthrown by the bare hands of the

[666] James Griffiths, 'China Is Exporting the Great Firewall as Internet Freedom Declines around the World' (*CNN*, 2 November 2018) <https://www.cnn.com/2018/11/01/asia/internet-freedom-china-censorship-intl/index.html> accessed 9 July 2019.

[667] Financial crisis of 2008 sparked protests against poor economic conditions and social inequality, particularly in Iceland, Spain, and the US.

people'.[668] Citizens were armed not with weapons but with Web 2.0 capacities. The voices of a few were joined immediately by the voices of thousands, online discontent quickly turned into offline protests, and 'hot spots' of this nature appeared simultaneously around the world. Naturally, this trend was viewed with trepidation by authoritarian governments in the post-Soviet region as they fought to maintain power. Moreover, this fear was fuelled by the local revolutions and changes of governments during the previous decades, as described above: for instance, the Colour Revolutions in Georgia (2003), Ukraine (2004), and Kyrgyzstan (2005), and Ukraine's Euromaidan in 2014.

As a response to the growing threat of social unrest, the governments under scrutiny in the present study increased their ability to block unwanted content. This refers here in particular to Russian, Belarusian, Kazakhstan, Kyrgyzstan, Azerbaijan, and Uzbekistan legal practices. However, recent developments in Ukraine – the blocking of Russian social media and websites – are also of considerable concern.[669]

The data from this study demonstrate commonalities in the approach of the above-mentioned countries with regard to blocking without judicial supervision (including 'umbrella' blacklists), overzealous blocking, establishing editorial responsibility for online media and bloggers, and intermediary liability. A large number of legislative developments in recent years have been devoted to Internet sources, which the author will cover in detail in the following sections. For instance, Kazakhstan in 2009 declared all online sources to be media outlets. In 2010, Belarus introduced the licensing of Internet resources under

[668] Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (John Wiley & Sons 2015) 1.

[669] Oleg Soldatov, 'Is the Ukrainian ban on Russian social media justified?' (*European Centre for Press and Media Freedom*, 1 August 2018) <http://www.rcmediafreedom.eu/Tools/Legal-Resources/Is-the-Ukrainian-ban-on-Russian-social-media-justified> accessed 21 June 2019.

presidential decree No. 60,[670] while Media Law amendments of 2014[671] and 2018[672] expanded governmental control over online content even further. Since 2013,[673] Russian lawmakers have adopted a series of legislative packages granting the state regulator, Roskomnadzor, extensive authority to block websites that are considered undesirable.

In theory, such legislative provisions seem to be a positive development to protect netizens on a national level and to regulate illegal content. In practice, however, given the repressive nature of regulations relating to the media environment, the amendments seem nothing more than a tool to crack down on online speech. As Morris observed with regard to media freedom across former Soviet states, 'having already brought traditional media to heel, authoritarian leaders are now focused on the few remaining spaces for free expression – particularly the Internet'.[674] This is confirmed by the fact that on a number of occasions the blocking procedure lacks transparency,[675] an extensive amount of legal content is affected 'by mistake',[676] and hundreds of Internet users are held liable on the basis of broadly worded charges and bizarre accusations.[677]

---

[670] Andrei Richter, 'Commentary on the Decree of the President of the Republic of Belarus "On Measures to Improve the Use of the National Segment of the Internet"' (OSCE 2010) <https://www.osce.org/fom/67911?download=true> accessed 10 July 2019.

[671] New media regulation enables the blocking of websites without a court approval even for a one-time violation. See Bastunets (n 555).

[672] Social networks can be banned extrajudicially. See 'Popravki v Zakon o SMI: registratsiya internet-izdaniy, identifikatsiya kommentatorov, blokirovka sotssetey [Amendments to the Law on Mass Media: registration of Internet publications, identification of commentators, blocking of social networks]' (*BAJ*, 6 April 2018) <https://baj.by/be/content/popravki-v-zakon-o-smi-registraciya-internet-izdaniy-identifikaciya-kommentatorov-blokirovka> accessed 22 June 2019.

[673] Federal Law 'On Amending the Federal Law 'On Information, Information Technologies and Protection of Information' 2013 [398-FZ].

[674] Morris (n 523).

[675] For instance, in Belarus only the Communication Ministry, law enforcement agencies, and service providers have access to the Internet blacklist.

[676] See Section 6.2.5, *'Cases where entire platforms – not just pages – have been blocked'*.

[677] Due to the broad interpretation of 'extremism', several Internet users in Russia were held liable for posting religious-themed memes. See Olga Robinson, 'The Memes That Might Get You Jailed in Russia' (23 August 2018) <https://www.bbc.com/news/blogs-trending-45247879> accessed 10 July 2019.

Muižnieks emphasised deficiencies with regard to arbitrary blockings in several states under scrutiny – Russia, Azerbaijan, and Ukraine. According to him, not the least risk with respect to banning online sources is that once authorities have blocked legitimate targets – e.g. child pornography − they follow any other content of which they disapprove.[678]

In contrast, not all sub-regional groups are experiencing strict online content regulations. For instance, in Georgia, Armenia and Estonia,the blocking and filtering of the Internet is not carried out in a systematic manner.[679] As a result of this distinction, the states in question are referred to only briefly in the following sections.

6.2.1. Internet Blacklists

The evidence below suggests that since the late 2000s, authoritarian regimes across post-Soviet space have sought to limit online speech, and have granted more power to regulatory bodies to block unwanted websites. By and large, authorities have justified tightening regulation by emphasising the need to ensure national security and to protect citizens online, as described in detail in the previous section.

Legislative developments have been based on two requirements: the creation of official blacklists of web sources and provisions to block content without a court order.

An Internet blacklist is a list of web sources banned in a certain territory. Maintaining this type of registry is common practice in former Soviet republics, particularly in Russia and Belarus. For the purpose of further investigation, the technical implementation of blacklisting should be clarified. To put it simply, each device that is part of a network – a computer, a router, or a server hosting a website – is assigned a numeric IP (Internet Protocol) address

[678] Muižnieks (n 490).

[679] The author drew this conclusion in accordance with the recent Freedom House Reports. See, for instance, regional reports from 'Freedom on the Net 2018: The Rise of Digital Authoritarianism' (*Freedom House*, 30 October 2018) <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism> accessed 5 September 2019.

that contains information on the physical location of the device.[680] When a subscriber tries to enter a particular web page, the provider receives a request from the subscriber's IP address to access the website's IP address. Blocking IP addresses is the simplest way to block access to a web page on a certain territory: that is, when Internet Service Providers are ordered to deter the transfer of information from certain domain names and IPs. The banned addresses are added to blacklists that local ISPs are legally required to follow.[681]

The registries of forbidden online sources of information are typically maintained by government agencies, such as Roskomnadzor[682] in Russia or BelGIE[683] in Belarus. State communication regulators are authorised to blacklist online sources prior to or without court approval.[684]

As examples below show, banning was applied initially to explicitly illegal content such as pornography or violent speech. However, when the blocking rule was extended on the basis of vaguely defined legal categories – extremism and defamation, to name two[685] – this inevitably affected an extensive amount of legal content.

In its early stage, the list of restricted access sites in Belarus was implemented only in governmental facilities. In February 2010, the Belarusian President, Alexander Lukashenko, signed a decree introducing more aggressive control over the Internet.[686] In line with this decree, the Ministry of Telecommunications and the Presidential Administration's Operations and Analysis Center (OAC) issued a regulation enacting a blacklist of websites to be blocked

[680] Soldatov, 'The Russian VPN ban' (n 538).
[681] ibid.
[682] Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications.
[683] State Supervisory Department for Telecommunications of the Republic of Belarus.
[684] See Section 6.2.2, *'Mechanisms to block websites without judicial approval'*.
[685] See Section 6.1, *'Legitimising Limitations to freedom of expression in the post-Eastern bloc region: state security concerns'*.
[686] Decree of the President of the Republic of Belarus 'On measures to improve the use of the national segment of the Internet' 2010 [60].

in state organisations, educational and cultural facilities, and Internet cafés.[687] Service providers were required to block content from two lists: one is a publicly available list of websites registered in Belarus, whereas the other is open only to operators, and includes foreign web pages as well. Blocking in private households and businesses could be implemented following a personal request from citizens. According to the authorities' official position, the aim of the document was to protect citizens from harmful content such as pornography, extremism, or violence. Civil rights activists, however, stressed that the law had been developed to block opposition websites in the run-up to the elections.[688]

Soon afterwards, in March 2010, the Information and Communication Agency of Kazakhstan declared the formation of the 'Service to React to Computer Incidents', which would analyse 'destructive' websites and create a blacklist.[689] Details of the selection criteria were not specified, which raised concerns among advocates of free expression.[690]

In July 2012, Russian lawmakers approved amendments to the Law on Protecting Children.[691] The latter changes enabled Roskomnadzor (State Internet Regulator) to blacklist and block websites harmful to children, particularly those sources containing pornography or instructions on methods of suicide. Federal Law No. 398-FZ 'On amending Federal Law 'On Information, Information Technologies and Protection of Information'' from 28 December 2013 replenished the blacklist with new categories on extremism, on calling for illegal

---

[687] 'Freedom on the Net 2015: Belarus' (*Freedom House*, 27 October 2015) <https://freedomhouse.org/report/freedom-net/2015/belarus> accessed 21 June 2019; 'The list of restricted access' (*Belarusian State Telecommunications Inspectorate*) <https://belgie.by/ru/lists_access> accessed 21 June 2019.

[688] 'Podpisan Odioznyy Ukaz o Tsenzure Interneta [Odious Decree on Internet Censorship Signed]' (*Charter 97*, 1 February 2010) <https://charter97.org/ru/news/2010/2/1/25943/> accessed 21 June 2019.

[689] 'Freedom on the Net 2011: Kazakhstan' (*Freedom House*, 13 January 2012) 20 <https://freedomhouse.org/report/freedom-net/2011/kazakhstan> accessed 21 June 2019.

[690] 'Disdaining Press Freedom, Kazakhstan Undermines OSCE' (*Committee to Protect Journalists*, 14 September 2010) <https://cpj.org/reports/2010/09/disdaining-press-freedom-kazakhstan-undermines-osc.php> accessed 16 July 2019.

[691] The Law 'On Amendments to the Federal Law "On the Protection of Children from Information Harmful to their Health and Development" and certain legislative acts of the Russian Federation' 2012 [139-FZ].

gatherings, and on violating the established order.[692] The blockings are commonly performed with respect to sensitive topics involving the Kremlin's politics, and they target oppositional media outlets and Ukrainian news sources.[693] Over the past few years, owing to the vague formulations of the law, thousands of websites with legal content have been included in the registry.[694]

In contrast to blacklists in Belarus and Kazakhstan, Russia suggested an overall blocking mechanism rather than situational blocking. This example had a spillover effect on other post–Soviet states. For example, in 2012 Ukrainian officials did not preclude the possibility of maintaining a similar list.[695]

It is worth noting that the Russian Internet blacklist affected neighbouring countries on several occasions. The first incident occurred in Belarus in August 2014, when Ukrainian webpages listed in the registry became unavailable. Belarusian users received notifications that access was limited 'under the legislation of the Russian Federation'. Local activists requested clarification from the Ministry of Information and Beltelecom, and called upon them to restore access immediately. Soon afterwards, the websites resumed their work.[696] Yet another incident occurred in 2014, when, as a result of Roskomnadzor's bans, Armenian users were unable to access five websites.[697] For Armenia, this was not a one-time event, as the country partially receives traffic from Russian providers. In 2012, for instance, Armenian users were unable to enter Kavcazcenter.com – the site reporting on the Chechen conflict and

[692] See Section 6.1 for details on the over-use of anti-extremism legislation.
[693] See Section 6.1 for details on the over-use of anti-extremism legislation.
[694] Roskomsvoboda reports that 220,116 webpages were eventually unblocked, which proves that their content was legal. 'Raspredeleniye Blokirovok Saytov Po Vedomstvam [Distribution of Blocking Sites by Department]' (*Roscomsvoboda*) <https://reestr.rublacklist.net/visual/> accessed 21 June 2019.
[695] Olga Karpenko, 'V Ukraine takzhe mogut vvesti reyestr zapreshchennykh saytov [Ukraine may introsuce the register of prohibited sites]' (*AIN.UA*, 6 November 2012) <https://ain.ua/2012/11/06/v-ukraine-takzhe-mogut-vvesti-reestr-zapreshhennyx-sajtov/> accessed 21 June 2019.
[696] 'Freedom on the Net 2015: Belarus' (n 687).
[697] 'Freedom on the Net 2015: Armenia' (*Freedom House*, 27 October 2015) <https://freedomhouse.org/report/freedom-net/2015/armenia> accessed 22 June 2019.

news of the Islamic world, as it had been banned in Russia by a court decision.[698] Similarly, in July 2015, access to a Russian opposition site and a gambling site was blocked.[699]

Following the Russian lead, self-proclaimed territories in Eastern Ukraine (see above under *'Frozen conflicts and unrecognised territories on post-Soviet space'*) created their own Internet blacklists. De-facto authorities of the Donetsk People's Republic announced the later 'registry' on 30 May 2015.[700] According to reports, the list contained mainly Ukrainian news sources and national media outlets. Another unrecognised state, the Lugansk People's Republic, banned approximately 117 URLs to prevent the 'destabilising' influence of Ukrainian media.'[701]

After the 2013-2014 events referred to as 'Euromaidan' in neighbouring Ukraine, and in the upcoming Belarusian presidential elections, the state of Belarus strengthened the procedure for blocking online content. Dated 19 February 2015, Ruling 6/8 by the President's Operational Analytical Center and Telecommunication Ministry[702] covered the actions of all Belarusian Internet users, and not just government institutions, educational, and cultural institutions, as had been the case earlier.[703] The blacklisted websites were in fact blocked within the whole territory of Belarus. The blacklist was now maintained by the State

---

[698] Samvel Martirosyan, 'Armenia Subject to Censorship from Russia' (*Media.am*, 25 December 2012) <https://media.am/en/blocked-website-in-armenia> accessed 22 June 2019.

[699] Samvel Martirosyan, 'Ej.Ru and Bet365.Com Blocked by Russian Roskomnadzor in Armenia' (*Banman.am*, 3 July 2015) <https://www.banman.am/2015/07/ejru-and-bet365com-blocked-by-russian.html> accessed 22 June 2019.

[700] Tetyana Lokot, 'Self-Proclaimed "Donetsk People's Republic" Now Has an Internet Blacklist' (*Global Voices*, 17 June 2015) <https://globalvoices.org/2015/06/17/self-proclaimed-donetsk-peoples-republic-now-has-an-internet-blacklist/> accessed 21 June 2019.

[701] Tetyana Lokot, 'Ukrainian Separatists Block 100+ News Websites in "Lugansk People's Republic"' (*Global Voices*, 14 January 2016) <https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/> accessed 11 July 2019.

[702] Ruling 'On approval of the Regulations on the procedure for restricting access to information resources (their constituent parts) on the Internet' 2015 [6/8].

[703] Galina Petrovskaya, 'Belorusskiy segment interneta: pod kolpakom u gosudarstva [Belarusian segment of the Internet: under the hood of the state]' (*DW.COM*, 24 September 2015) <https://bit.ly/2JwWnhJ> accessed 21 June 2019; 'Belarusian Authorities Want to Completely Block Independent Websites' (*Charter 97*, 2015) <https://charter97.org/en/news/2015/2/25/140908/> accessed 21 June 2019.

Supervisory Department for Telecommunications of the Republic of Belarus, according to recommendations from the Information Ministry. Providers were obligated to check the list regularly and to block all websites shown on it. It should be noted that the registry was available only to providers and governmental entities. From 2018, the list of restricted websites became even more inaccessible. According to the latest procedure on blocking, the blacklist may be reviewed only by the Information Ministry, the Telecommunication Ministry, the bodies carrying out operational and investigative activities, the bodies of the Prosecutor's Office and the preliminary investigation, the bodies of the State Control Committee, and by tax authorities, courts, and ISPs.[704] This last update also eliminated the list of individuals and organisations that may complain about illegal information online. Initially, any Belarusian citizen or body of authority could initiate adding the particular website to the registry of restricted access. In 2018, however, this regulation was abandoned, leaving decisions to be carried out by the Information Ministry.

Compared to other post-Soviet countries, Ukraine is considered to have a more favourable climate as regards free expression. Nonetheless, in recent years the government has taken ambiguous steps to ensure state security amidst the conflict in the Eastern regions. A great deal of content filtering occurred with respect to pro-Russian opinions. Ironically, the initiatives at times were reminiscent of the Russian approach. By way of illustration, announcing a new cyber police unit in 2015, Ukraine's Interior Minister presented a plan to create a register of ‘forbidden’ websites. The blacklist would include child pornography websites as well as those containing pirated and malware material. The procedure of blocking, however, was unclear.[705] The next example is represented by the Decree of the President of Ukraine No. 133/2017, which introduced a long list of Russian websites to be

[704] Ruling ‘On the procedure for restricting (renewing) access to Internet resources’ 2018 [8/10/6].
[705] Tetyana Lokot, ‘Ukraine’s New Banned Websites Registry: Security Measure or Censorship Tool?’ (*Global Voices*, 22 October 2015) <https://globalvoices.org/2015/10/22/ukraines-new-banned-websites-registry-security-measure-or-censorship-tool/> accessed 21 June 2019.

blocked by ISPs. The sanction list included the most-used social media platforms VK and Odnoklassniki and the search engine Yandex. At the time of blocking, Alexa rankings placed the websites among the top ten most popular in Ukraine. Public opinion on the matter was divided. Some suggested that the measures were necessary to counter Russian aggression and propaganda, while others argued that the decree would reduce freedom of expression and the pluralism of opinions in the country.

The official line of reasoning on the blocking of Russian websites in Ukraine rested on two major arguments: 1) Russian social media share their Ukrainian clients' personal data and correspondence with Russian intelligence services; 2) considering the 'hybrid war' that Russia is waging against Ukraine, blocking is a matter of national security and is not targeting freedom of expression. In particular, such argumentation was given by the then President of Ukraine, Petro Poroshenko, in an online petition calling for an annulment of the decree,[706] as well as in an official reply of the Ukrainian government to a 'level 2 media freedom alert' on the Council of Europe Platform to promote the protection of journalism and the safety of journalists.[707] Nonetheless, non-governmental organisations highlighted the disproportionality of the measure, as blockings would affect a large section of legitimate content.[708]

[706] 'Otmenit' Blokirovku Internet-Resursa Vkontakte [Online Petition: To Cancel Blocking of the Internet Resource Vkontakte]' (*Official online representation of the President of Ukraine*, 29 June 2017) <http://petition.president.gov.ua/petition/36543> accessed 16 July 2019.
[707] 'Ukraine Blocks Russian Social Networks and Expands Economic Sanctions Against Russian Companies' (*Platform to promote the protection of journalism and safety of journalists*, 17 July 2017) <https://rm.coe.int/ukraine-en-reply-ukraine-blocks-russian-social-networks-and-expands-ec/168073254f> accessed 16 July 2019.
[708] Muižnieks (n 490).

Initially, the ban was introduced for three years. In March 2019, Petro Poroshenko prolonged sanctions for another term. In addition, it should be noted that the sanction list was extended in recent years to include more Russian companies.[709]

In the author's opinion, to comply with international standards of freedom of expression, the analysed states should ensure transparency in maintaining online blacklists. In 2011 for instance, Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, called for states to provide lists of banned webpages, along with 'full details regarding the necessity and justification for blocking'.[710] According to the Rapporteur, without transparency it would be difficult to define whether the filtering was necessarily for the purported aims.

6.2.2. Mechanisms to Block Websites Without Judicial Approval

As regards the second requirement of tightening the control of online content, several of the states analysed introduced legislation aimed at blocking websites without court approval. The authorities justify such provisions by emphasising the need to ensure national security; in practice, however, such measures violate international standards. Firstly, as the UN Special Rapporteur on Freedom of Expression stressed,

> *the determination of what content should be blocked must be undertaken by a competent judicial authority or a body that is independent of any political, commercial or other unwarranted*

[709] Olga Karpenko, 'Prezident zablokiroval «Yandeks» v Ukraine yeshche na tri goda. I ryad drugikh IT-kompaniy [The president blocked Yandex in Ukraine for another three years. And a number of other IT companies]' (*AIN.UA*, 20 March 2019) <https://ain.ua/2019/03/20/opyat-blokiruetsya-yandeks-v-ukraine/> accessed 21 June 2019; Denis Vergun, 'V Ukraine Zablokiruyut Yeshche 180 Saytov – SBU Nastaivayet [180 More Sites Will Be Blocked in Ukraine - SBU Insists]' (*UBR*, 13 July 2018) <https://ubr.ua/market/telecom/v-ukraine-zablokirujut-eshche-180-sajtov-sbu-nastaivaet-3873006> accessed 21 June 2019.

[710] Frank La Rue Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (n 424) para 70.

> *influences in order to ensure that blocking is not used as a means of censorship*.[711]

Secondly, online regulations within the region fall outside of legitimate restrictions: for example, child pornography or the inciting of terrorism, which are recognised universally by international law. Instead, the states under scrutiny try to regulate online expression in the interest of stifling dissent.[712] For instance, in recent years in Russia 'thousands of sites were blocked by mistake'.[713]

Since December 2013, the General Prosecutor's Office in Russia has been granted the authority to directly order the blocking of access to illegal content by way of 'Lugovoy's Law'.[714] Therefore, web pages 'suspected of extremism', 'calling for illegal meetings', 'inciting hatred', and 'violating the established order' may be blocked without a judicial decision.[715] Furthermore, it should be noted that blocking is carried out by service providers, whereas website owners are notified of the ban post factum.[716] It has been mentioned in the present section that amendments resulted in the successful blocking of Ukrainian media and Russian opposition websites.[717]

Legislative amendments during the Yanukovich regime,[718] made in Ukraine in the midst of the Euromaidan events, also included a provision on extrajudicial blocking. In this manner, independent media outlets were targeted under violations regarding extremism, but the law was repealed by the new government.

---

[711] La Rue F, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 2011 [A /66/290].
[712] Morris (n 523).
[713] Soldatov and Borogan (n 120) 313.
[714] Federal Law 'On Amending the Federal Law 'On Information, Information Technologies and Protection of Information' (n 673).
[715] 'Russian Efforts At Internet Censorship' (n 547).
[716] Pollicino and Soldatov, 'Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (n 454).
[717] See Section 6.1 for details on the over-use of anti-extremism legislation.
[718] Ibid.

In April 2014, Kazakhstan introduced the Law 'On Amendments and Addenda to Laws Governing the Activity of Internal Affairs Bodies'. New regulations authorised the General Prosecutor to suspend the activities of websites without court approval. The law stipulated the blocking of content that called for extremism, unauthorised public gatherings, or mass riots.[719]

In 2014, Belarusian lawmakers updated the Media Law, which significantly extended the Information Ministry's authority to regulate online content. Webpages may be banned if they have received two warnings within 12 months, or even for first-time violations.[720] In addition, the Ministry is authorised to conduct the extrajudicial blocking of websites. The law applies to extremist, pornographic, or violent content, and to publications containing propaganda relating to war or that is harmful to national interests.

Kazakhstan amended the Law on Communications in 2016. With a further view to preventing crimes, the National Security Committee was empowered to block Internet networks and means of communication without a court decision. The committee was only required to notify authorised bodies within 24 hours.[721]

The Azerbaijani 'Law on Information, Informatisation, and the Protection of Information' was amended in 2017. The relevant authorities were empowered to block a website within eight hours if they detected content considered to be dangerous to the state or to society. In this case, the responsible body was required to notify an editor of the page and to obtain judicial approval only after the fact. New provisions enabled authorities to block

[719] Law of the Republic of Kazakhstan 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan Concerning the Activities of the Internal Affairs Bodies' 2014 [200–V].
[720] Bastunets (n 555).
[721] Law of the Republic of Kazakhstan 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Countering Extremism and Terrorism' (as amended on February 27, 2017) 2016 [28–VI]; Adil Nurmakov, 'Siloviki Kazakhstana poluchat polnomochiya po otklyucheniyu svyazi [Security forces of Kazakhstan will be authorized to disable communication]' (*Digital Report*, 14 October 2016) <https://digital.report/siloviki-kazahstana-smogut-otklyuchat-svyazi/> accessed 27 June 2019.

several independent media, including Radio Free Europe/Radio Liberty, Meydan TV, and the Organised Crime and Corruption Reporting Unit (OCCRP) page.[722]

In July 2017, deputies in Ukraine suggested two bills to protect national security. The draft law contained normative provisions empowering the authorities to ban websites without judicial approval within 48 hours.[723] This legislative initiative received harsh criticism from local civil society,[724] owing to the broad provisions that grant authorities unlimited power to block Internet sources of information. The Ukrainian parliament did not approve the amendments, although the presidential decree of 2017 banned a number of Russian websites in Ukraine.[725]

In 2018, Belarus introduced even more restrictive amendments to the Media Law. The new law allows, *inter alia*, the possibility of blocking social networks without warning or court approval. The article is formulated as follows:

> *If there is no technical possibility to implement a decision on restricting access to an integral part of an Internet resource and on the owner's failure to accept an Internet resource in terms established by the republican government body in the field of mass*

---

[722] Arzu Geybulla, 'Azerbaijan's Blocking of Websites Is a Sign of Further Restrictions Online' (*openDemocracy*, 31 August 2018) <https://www.opendemocracy.net/en/odr/azerbaijans-blocking-of-websites/> accessed 22 June 2019; 'Online Censorship Rounds off Aliyev's Control of Azerbaijani Media' (*RSF*, 3 May 2017) <https://rsf.org/en/news/online-censorship-rounds-aliyevs-control-azerbaijani-media> accessed 22 June 2019.

[723] Mariana Zakusylo, 'Deputaty khochut′ uzakonyty dosudove blokuvannya internet-resursiv [MPs want to legalize extra-judicial blocking of internet resources]' (*detector.media*, 12 July 2017) <https://detector.media/infospace/article/127856/2017-07-12-deputati-khochut-uzakoniti-dosudove-blokuvannya-internet-resursiv/> accessed 22 June 2019.

[724] Digital Security Lab, 'Legal Analysis of the Draft Law "On Amending Certain Laws of Ukraine on Countering Threats to National Security in Information Sector," Registration #6688' (*Medium*, 2 July 2018) <https://medium.com/@cyberlabukraine/legal-analysis-of-the-draft-law-on-amending-certain-laws-of-ukraine-on-countering-threats-to-39b3738d97cf> accessed 22 June 2019; Oksana Grytsenko, 'Parliament Committee Okays Bill Critics Say Will Block Websites, End Internet Anonymity' (*KyivPost*, 5 July 2018) <https://www.kyivpost.com/ukraine-politics/parliament-committee-okays-bill-critics-say-will-block-websites-end-internet-anonymity.html> accessed 22 June 2019.

[725] See Section 6.2.1, *'Internet blacklists'*.

> *information, or on measures to remove information contained in an Internet resource, the republican government body in the field of mass media has the right to decide on restricting access to the information resource as a whole.*[726]

With regard to the current section, the author suggests that analysed states should revise the practice of extrajudicial blocking. International standards generally require the states to ensure that restrictions be imposed by an independent adjudicatory body, and the decision on blocking must provide for appellation. Nils Muižnieks, Council of Europe Commissioner for Human Rights, notes that the states should guarantee judicial supervision, whereas domestic courts are required to determine whether the restriction is necessary and proportionate.[727] International human rights organisation Article 19 recommends that blocking only be ruled by courts, and relevant intermediaries should have the possibility of contesting the decision.[728] The *Joint Declaration on Media Independence and Diversity in the Digital Age* calls for the states to ensure that national security provisions are applied clearly and narrowly, as well as their examination by a court.[729]

6.2.3. Labelling and Targeting Foreign Websites as 'Foreign Agents'

In October 2011, Belarusian lawmakers secretly passed amendments criminalising foreign funding for NGOs.[730] Because most independent media outlets operated as non-

[726] 'Popravki v Zakon o SMI: registratsiya internet-izdaniy, identifikatsiya kommentatorov, blokirovka sotssetey [Amendments to the Law on Mass Media: registration of Internet publications, identification of commentators, blocking of social networks]' (n 672).
[727] Muižnieks (n 490).
[728] 'Freedom of Expression Unfiltered: How Blocking and Filtering Affect Free Speech' (Article 19 2016) 20.
[729] 'Joint Declaration on Media Independence and Diversity in the Digital Age' (n 532) para 3.f.
[730] 'Freedom on the Net 2012: Belarus' (*Freedom House*, 17 September 2012) <https://freedomhouse.org/report/freedom-net/2012/belarus> accessed 23 June 2019.

government organisations, legislative changes entailed considerable risk with regard to freedom of speech.[731]

The term 'foreign agent' was introduced for the first time in Russian legislation in 2012. The law defined as such all non-governmental organisations taking part in political activities and receiving foreign funding.[732] Since then, the term has been used widely within the post-Soviet region.

Anti-protest amendments during Yanukovych's administration contained, *inter alia*, the provision on defining foreign-funded NGOs as 'foreign agents'.[733]

In a comparable manner, Azerbaijan updated the law on grants in February 2014. President Aliyev signed amendments targeting NGOs funded by outside sources. The changes empowered the government to strengthen control over independent media and society. As for the media, Aliyev approved even more restrictive measures in February 2015. Updated media law authorised courts to close foreign-funded media if they were found to be responsible for an incident involving defamation twice in a year. New regulations resulted in difficulties receiving foreign grants, and therefore a number of independent websites ceased their activities in Azerbaijan. The list includes Channel 13, Mediaforum, Zerkalo/Ayna, Obyektiv TV, and the Azerbaijani service of the Radio Free Europe/Radio Liberty.[734]

---

[731] 'Belarus: Open Joint NGO Letter to the Parliament of Belarus' (*Human Rights Watch*, 20 October 2011) <https://www.hrw.org/news/2011/10/20/belarus-open-joint-ngo-letter-parliament-belarus> accessed 23 June 2019.

[732] The Law 'On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of the Activities of Non-Profit Organizations Acting as a Foreign Agent' 2012 [121-FZ].

[733] Pavel Polityuk and Richard Balmforth, 'Ukraine Parliament Pushes through Sweeping Anti-Protest Law' *Reuters* (16 January 2014) <https://www.reuters.com/article/us-ukraine-law-idUSBREA0F12M20140116> accessed 23 June 2019; 'Yanukovych Commits Ukraine to Authoritarian Path' (n 552).

[734] 'Yet Another Intimidatory Signal to Independent News Media' (*RSF*, 10 February 2015) <https://rsf.org/en/news/yet-another-intimidatory-signal-independent-news-media> accessed 23 June 2019; 'Freedom on the Net 2017: Azerbaijan' (n 638).

Russia passed the law on 'undesirable organisations' in May 2015.[735] This legislative update enabled the General Prosecutor's Office to announce foreign CSOs as being 'undesirable' if they were considered a danger to national security. Subsequently, in 2017, the law targeted five websites connected to Open Russia – a non-government organisation run by Kremlin opponent Mikhail Khodorkovsky – as well as the websites of the National Democratic Institute and other independent organisations.[736]

In November 2017, Russia introduced a new piece of legislature *vis-à-vis* international media outlets.[737] The law requires foreign-funded mass media to be registered as 'foreign agents'. The list of outlets, including Radio Free Europe/Radio Liberty international and local services, including the Voice of America, were put in this category.[738]

Limiting the operation of independent organisations in those countries with a fragile rule of law and a poor human rights environment may pose a serious threat to freedom of expression, the media, and other associated rights. Governments should take into account that the ability to receive grants, donations, and other funding is essential for human rights organisations to carry out their activities, as well as to freely communicate with the most vulnerable social groups and minorities. Moreover, the practice of labelling organisations as 'foreign agents' creates unnecessary obstacles for international corporations, and facilitates a biased attitude on the part of citizens as well as with regard to the selective applicability of regulations by authorities. Therefore, the revision of approaches towards foreign organisations in analysed regions would represent progressive development in accordance with standards involving human rights.

---

[735] Federal Law 'On Amendments to Certain Legislative Acts of the Russian Federation' 2015 [129-FZ].
[736] 'Freedom on the Net 2018: Russia' (n 540).
[737] Federal Law 'On Amending Articles 10.4 and 15.3 of the Federal Law on Information, Information Technologies and Protection of Information and Article 6 of the Law on Mass Media 2017 [327-FZ].
[738] 'EU Criticizes Russia's "Foreign Agents" Media Law' (*RadioFreeEurope/RadioLiberty*, 26 November 2017) <https://www.rferl.org/a/russia-putin-signs-foreign-agent-media-law-rferl-voa-cnn-deutsche-welle/28876680.html> accessed 23 June 2019; 'Freedom on the Net 2018: Russia' (n 540).

6.2.4. Blogger Responsibility

A worrisome increase in legislative initiatives − often in the guise of 'protecting national security' − to crack down severely on the online expression of private individuals is also evident in the countries under scrutiny. As shown in examples below, authorities have sought to impose media requirements not only on online news platforms but also on bloggers.

As early as July 2009, the President of Kazakhstan, Nursultan Nazarbayev, approved amendments to communication law.[739] All Internet sources – including web forums, blogs, chats, and Internet TV – were defined as mass media and subjected to the same legal responsibility. The webpages – irrespective of whether their servers and domains were located in Kazakhstan or abroad – may be banned if they contain propaganda involving a violent change to the constitutional system; violation of the integrity of the Republic of Kazakhstan; undermining of the security of the state; propaganda concerning extremism or terrorism; or the inciting of ethnic and inter-confessional enmity, and so on.[740]

From August 2014 until July 2017, the 'Bloggers' Law'[741] was in force in Russia. Under this law, bloggers with more than 3000 readers per day were required to obtain governmental registration, and to disclose their real identity.[742] Online writers were included in a Bloggers' Register, and fell under same regulations as the state media. In particular, blogs on the list were required to contain details of the author's real name and contact

[739] The Law 'On amendments to some legislative acts of the Republic of Kazakhstan on information and communication networks' 2009 [178–IV].
[740] 'Fact Sheet - Human Rights in Kazakhstan' (*Human Rights Watch*, 18 November 2009) <https://www.hrw.org/news/2009/11/18/fact-sheet-human-rights-kazakhstan> accessed 2 July 2019; 'Parlament prinyal zakon, usilivayushchiy kontrol' nad internet-resursami v Kazakhstane [Parliament passed a law strengthening control over Internet resources in Kazakhstan]' (*Zakon.kz*, 24 June 2009) <https://www.zakon.kz/141606-parlament-prinjal-zakon-usilivajushhijj.html> accessed 2 July 2019.
[741] Federal Law 'On Amending the Federal Law "On Information, Information Security and Data Protection" and Certain Legislation of the Russian Federation Concerning the Exchange of Information Using Telecommunication Networks' 2014 [97-FZ].
[742] Neil MacFarquhar, 'Russia Quietly Tightens Reins on Web With "Bloggers Law" - The New York Times' (*New York Times*, 5 June 2014) <https://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html?_r=0> accessed 2 July 2019.

information. Other regulations imposed on popular bloggers obligated them to a) verify information before publishing it; b) abstain from releasing reports containing slander, hate speech, extremist calls, or other banned information such as, for example, advice regarding suicide; c) abstain from using obscene language; and d) follow electoral agitation guidelines.[743]

Violation of the law was punishable by heavy fines, with a maximum of €13 000 at the time the law came into force. The regulations affected numerous Internet users in Russia. As of 2014, there were approximately 500 Russian bloggers according to data from LiveInternet web counter.[744] The owner of LiveInternet also suggested that about 1,500 Russian-speaking Facebook users exceeded the audience of 3,000 unique daily readers. Although the intention behind the law may have been to balance freedom of expression and other fundamental rights, in practice the vague definitions of 'extremism', 'obscene language,' and other key terms provided for overly broad and arbitrarily implications.[745] Another critical point with respect to the law had to do with limiting the possibility of anonymous/pseudonymous blogging in Russia[746] and unclear estimates regarding daily audiences.[747] In addition, whereas the law placed the bloggers under the same obligations as officially employed journalists, it did not guarantee the same level of protection: namely, the right to retain the confidentiality of information sources. In the author's opinion, the latter issue may be extrapolated for all cases in the present section.

---

[743] Oleg Soldatov, 'Half-Hearted Inception, Miserable Existence, and the Untimely Death of the Bloggers' Register in Russia' (2019) 52 Israel Law Review 61.

[744] LiveInternet − the major blogging platform in Runet, which also provides a service on web statistics. See ibid.

[745] ibid.

[746] Even if there were a remote possibility that a blog would attract 3000 readers per day, the writer had to register with Roskomnadzor and provide contact details. See ibid.

[747] The number could be affected by visits from search engine bots, repeat visits from same users, DDoS–attacks, and so on. See ibid.

From a practical perspective, implementation of the law turned out to be problematic and ineffective, which ultimately caused Russian authorities to revise their online regulatory approach.[748] Commenting on the registry, Roskomnadzor's Head, Aleksandr Zharov, admitted that 'laws are not always as effective as they were at the time of their adoption, and law enforcement proves that laws require correction'.[749]

Uzbekistan lawmakers strengthened regulations regarding bloggers and freelance citizen journalists in August 2014, but shortly thereafter Russia's 'Blogger's Law' came into force. According to an amended Law on Informatisation, online writers in Uzbekistan are required to remove content if requested by the state. The law contains an overly broad implication of the term 'blogger'. Thus, any person spreading information on socio-political issues falls under the definition. Bloggers were obliged to ensure the credibility of publicly accessible information,[750] even if reposting content from other users. In the event that credibility was not proven, publications were to be removed immediately.[751] Moreover, bloggers were required to abstain from the dissemination of information containing propaganda regarding war, violence and terrorism, religious extremism, the inciting of hatred, and calling for a change to an existing constitutional order, and so forth.[752]

In 2014, OSCE Representative on Freedom of the Media, Dunja Mijatović, expressed concern with respect to such requirements for bloggers. The Representative stressed that the restrictions go far beyond the admissible limits of free speech expressed in the OSCE commitments and other international standards.[753]

---

[748] ibid.
[749] 'Roskomnadzor zakryl reyestr populyarnykh blogerov [Roskomnadzor Shut Down the Bloggers' Register]' (*NTV*, 1 August 2017) <https://www.ntv.ru/novosti/1880680/?fb> accessed 25 July 2019.
[750] Article 12.1
[751] Law of the Republic of Uzbekistan 'On introducing amendments to some legislative acts of the Republic of Uzbekistan' 2014 [ЗРУ-373-son].
[752] ibid Art 12(1).
[753] Dunja Mijatović, 'New Restrictions in Uzbekistan Further Limit Free Expression on Internet, OSCE Representative Says' (*OSCE*, 8 September 2014) <https://www.osce.org/fom/123275> accessed 19 July 2019.

6.2.5. Cases Where Entire Platforms – Not Just Pages – Have Been Blocked

Commenting on the issue of arbitrary blockings in Council of Europe member states, the Commissioner for Human Rights, Nils Muižnieks, noted the growing number of overblocking cases in the Russian Federation (that is, when a ban affects websites not targeted originally).[754] The legal system in place inevitably leads to 'false positives' when regulators block an extensive amount of legal content. For instance, approximately 226,000 websites in Russia were falsely included in a blacklist by July 2019.[755] The prominent web platforms, such as Wikipedia and YouTube, were at some point affected by the vague requirements of Russian law.[756]

Cases of overblocking occurred in other states under scrutiny. Authorities targeted content threatening national security or citizens; however, due to the lack of technical capacities[757] to perform selective bans, regulators closed websites entirely.

In October 2008, the prominent blogging website LiveJournal became inaccessible in Kazakhstan. At that time, nearly 230,000 Kazakh users were active on the service – nearly the third of all Russian-language bloggers.[758] Local bloggers assumed that blocking had been carried out by the national ISP 'Kazakhtelecom'. The provider, however, never confirmed that blocking had taken place, saying the problem was the result of technical issues at LiveJournal.

---

[754] Muižnieks (n 490).

[755] 'Raspredeleniye Blokirovok Saytov Po Vedomstvam [Distribution of Blocking Sites by Department]' (n 718).

[756] Tetyana Lokot, 'Russia's Internet Watchdog May Soon Get More Extrajudicial Website Blocking Powers' (*Global Voices Advocacy*, 11 November 2015) <https://advox.globalvoices.org/2015/11/11/russias-internet-watchdog-may-soon-get-more-extrajudicial-website-blocking-powers/> accessed 21 July 2019.

[757] In most cases, governments implement blockings on IP addresses, which makes it difficult to block separate page. See Section 6.2.1, *'Internet blacklists'*.

[758] 'Human Rights in Kazakhstan: Seven Months before the OSCE Chairmanship' (*Human Rights Watch*, 20 May 2009) <https://www.hrw.org/news/2009/05/20/human-rights-kazakhstan-seven-months-osce-chairmanship> accessed 22 June 2019.

It is possible that LiveJournal was banned due to the opening of a new blog by Rakhat Aliyev, former son-in-law of the President of Kazakhstan, Nursultan Nazarbayev. After falling out with the President, Aliyev lived in exile in Austria after being found guilty of kidnapping and several other grave crimes in Kazakhstan.[759] According to Aliyev, the charges against him were politically motivated. Following these events, he launched an information-related campaign against President Nazarbayev. Publications in Alyiev's LiveJournal described, *inter alia*, 'attempts' on his life and 'massive secret arrests' in Kazakhstan.

Notably, the LiveJournal ban affected Kyrgyzstan users as well.[760] Experts suggested that the platform was inaccessible due to blockings in a neighbouring country, since the issues were only experienced by local providers that used connections through Kazakhtelecom.

Kazakh authorities banned LiveJournal for the second time in August 2011, as the court had concluded that the account *www.islamunveiled.livejournal.com* was spreading propaganda regarding terrorism, religious extremism, and public incitement to commit acts of terrorism.[761] A complaint in relation to the blog and 13 other websites was filed by the Astana City Prosecutor. The Russian blogging service Liveinternet.ru was blocked under the same violations.[762]

The representatives of LiveJournal's Russian branch stressed that Kazakh authorities had never contacted them with the request to remove 'extremist' material. Therefore, the

---

[759] ibid.

[760] '«Blokirovka ZHZH»: prichina «v provayderakh Kazakhstana», govoryat spetsialisty ["LJ blocking": the reason is "in the providers of Kazakhstan," experts say]' (*KLOOP.KG*, 10 October 2008) <https://kloop.kg/blog/2008/10/10/blokirovka-zhzh-prichina-v-provajderax-kazaxstana-govoryat-specialisty/> accessed 22 June 2019.

[761] Adil Soz Foundation, 'LiveJournal Portal, Several Blogs Suspended' (*IFEX*, 2 September 2011) <https://ifex.org/livejournal-portal-several-blogs-suspended/> accessed 22 June 2019.

[762] 'Freedom on the Net 2012: Kazakhstan' (*Freedom House*, 18 September 2012) <https://freedomhouse.org/report/freedom-net/2012/kazakhstan> accessed 21 July 2019.

platform owners were not aware of what had caused the suspension. The Kazakh state's civil rights organisation, Adil Soz, stressed that,

> *The Court decision to ban the whole portal violates the right of Internet users to access information and to disseminate information freely. The decision to ban the whole portal can be compared to the arrest of a whole family for the crime of one of its individual members.*[763]

Blogger Anatoly Utbanov tried to appeal the court's decision, claiming that blocking an entire platform was a disproportionate response with regard to just one blog containing illegal material. However, in March 2012, the Yessil District Court rejected the claim of the defendant.[764] According to a representative of the Ministry of Communication and Information, at the time there was no technical ability to block separate accounts, but it was claimed that such a system might be in place by July 2012.[765] The LiveJournal blocking lasted until November 2015, when the company agreed to the request to delete illegal material.[766]

In November 2012, the satirical platform Absurdopedia was added to the Russian list of forbidden websites.[767] Absurdopedia is the Russian branch of the international satirical wiki-encyclopaedia[768] Uncyclopedia, a parody analogue of Wikipedia. The source contains

---

[763] Adil Soz Foundation (n 761).
[764] *Decision of Yessil district court of Astana* [2012] Yessil district court of Astana 2-122/11.
[765] 'Sud podtverdil zakonnost' blokirovki ZHZH [Court confirmed legitimacy of LiveJournal's block]' (*Zakon.kz*, 18 April 2012) <https://www.zakon.kz/4485779-sud-podtverdil-zakonnost-blokirovki-zhzh.html> accessed 21 July 2019.
[766] 'Dostup k LiveJournal vosstanovlen v Kazakhstane [Access to LiveJournal recovered in Kazakhstan]' (*Tengrinews.kz*, 11 November 2015) <https://tengrinews.kz/internet/dostup-k-LiveJournal-vosstanovlen-v-kazahstane-283868/> accessed 21 July 2019.
[767] See Section 6.2.1, *'Internet blacklists'*.
[768] Wiki is a site where users can collectively modify content. The widely known platform running on wiki is Wikepedia, as well as other Wikimedia Foundation projects . See Michael Aaron Dennis, 'Wiki: Web Site'

articles written in a humorous manner, in formats ranging from satire to non-sequiturs and black humour. Absurdopedia was blacklisted for its satirical content on methods of suicide.[769] However, the blocking affected many more pages. Stanislav Kozlovsky, executive director of Russian Wikimedia, reported that providers blocked all of the encyclopaedias on wikia.[770] In the same week, the Russian state regulator blocked another popular satirical source, Lurkmore, a compendium of articles on Internet culture and memes.[771] The reason appeared to be that the article involved drugs. Both platforms – Absurdopedia and Lurkmore – were blocked as soon as they deleted the offending material.

Returning to the Kazakh practice, the blockings for state-security reasons are imposed on all kinds of web platforms, including world-renowned stock-photo agencies as well as video- and photo-hosting services.[772] For instance, the Kazakhstan government blocked the whole music platform SoundCloud in May 2015. The service presumably contained one account with Hizb-ut-Tahrir extremist materials.[773] By the end of June, SoundCloud had been restored. Moreover, in September 2015, the Yessil District Court ruled to block the Vimeo video platform and a dozen other pages allegedly carrying extremist content.[774] Access was restored in October 2015, when Vimeo deleted the video material in question.[775] In 2016, the

---

(*Encyclopedia Britannica*) <https://www.britannica.com/topic/wiki> accessed 21 July 2019; 'Wikimedia Foundation Governance Wiki' <https://foundation.wikimedia.org/wiki/Home> accessed 21 July 2019.

[769] 'Absurdopedia / Wikia' (*Roskomsvoboda*, 11 November 2012) <https://roskomsvoboda.org/3323/> accessed 21 July 2019.

[770] ibid.

[771] Andrey Tselikov, 'Lurkmore or Lurkless? The Russian Internet Blacklist In Action' (*Global Voices*, 14 November 2012) <https://globalvoices.org/2012/11/14/lurkmore-or-lurkless-the-russian-internet-blacklist-in-action/> accessed 21 July 2019.

[772] Dina Baidildayeva, 'Internet Censorship in Kazakhstan: More Pervasive than You May Think' (*openDemocracy*, 26 March 2018) <https://www.opendemocracy.net/en/odr/internet-censorship-in-kazakhstan/> accessed 21 July 2019.

[773] 'Freedom on the Net 2016: Kazakhstan' (*Freedom House*, 10 November 2016) <https://freedomhouse.org/report/freedom-net/2016/kazakhstan> accessed 22 June 2019.

[774] 'Vimeo.com zablokirovan v Kazakhstane [Vimeo.com is blocked in Kazakhstan]' (*Tengrinews.kz*, 22 September 2015) <https://tengrinews.kz/kazakhstan_news/Vimeocom-zablokirovan-v-kazahstane-281282/> accessed 22 June 2019.

[775] Meruert Nurgazinova, 'Rabota internet-resursa Vimeo v Kazakhstane vozobnovlena [The work of the Internet resource Vimeo renewed in Kazakhstan]' (*Kazpravda.kz*, 14 October 2015)

microblogging website Tumblr was banned due to extremist-related and pornographic accounts.[776]

In a manner similar to the above cases, all WordPress sites were blocked in Georgia in November 2015. The State Security Service detected a page with pro-Islamic State group videos.[777] However, the ban lasted for only a short period. In 2016, Georgian authorities partially blocked the YouTube and Vimeo websites. The incidents were related to sex videos involving Georgian politicians.[778] In both cases, access was restored within several hours.

On numerous occasions, Kazakh authorities denied the cases of blockings or refused to provide an explanation for them. For instance, on January 2017 an online petition platform Avaaz.com became inaccessible to local users. The incident occurred shortly after a petition against the temporary registration of citizens was launched on the platform.[779] The new legal provisions required citizens travelling within the country to register with local authorities if they remained in one locality for more than one month.[780] State officials did not provide any information as to why the site became inaccessible. The local civil rights organisation, Adil Soz, mentioned a case among the unsubstantiated blockings of the Internet within Kazakhstan. Overall, the organisation reported nine cases involving groundless limitations to online content between January and December 2017. The cases involved issues of access to

---

<https://www.kazpravda.kz/news/tehnologii/rabota-internet-resursa-vimeo-v-kazahstane-vozobnovlena> accessed 21 July 2019.

[776] 'Servis Tumblr Zablokirovali v Kazakhstane Iz-Za Propagandy Terrorizma i Pornografii [Tumblr Service Blocked in Kazakhstan Due to Propaganda of Terrorism and Pornography]' (*Tengrinews.kz*, 11 April 2016) <https://tengrinews.kz/internet/servis-Tumblr-zablokirovali-kazahstane-iz-za-propagandyi-292453/> accessed 22 June 2019.

[777] 'Freedom on the Net 2016: Georgia' (n 583).

[778] ibid.

[779] 'V Kazakhstane Zablokirovali Sayt s Petitsiyey Protiv Vremennoy Registratsii [Kazakhstan Blocked Website with Petition against Temporary Registration]' (*Tengrinews.kz*, 9 January 2017) <https://tengrinews.kz/kazakhstan_news/kazahstane-zablokirovali-sayt-petitsiey-protiv-vremennoy-309646/> accessed 22 June 2019.

[780] Aigerim Toleukhanova, 'Kazakhstan: Registration Law Causes Chaos, Forces Apology' (*Eurasianet*) <https://eurasianet.org/kazakhstan-registration-law-causes-chaos-forces-apology> accessed 21 July 2019.

social networks and messengers such as WhatsApp, Facebook, and Instagram.[781] Over the last decade, Kazakh users have repeatedly noted issues of connectivity to legitimate online content, and which have remained without an official explanation.[782]

The Kyrgyzstan court ruled to block the entire platforms JustPaste.it and Internet Archive in July 2017. These sites enabled access to deleted webpages that contained articles normally banned in the country.[783] An official from Kyrgyzstan's state communications service stated that the court had blocked the website due to 'extremist content' stored there, but did not specify when the court ruling was issued and what specific webpages had triggered the block. Local activists linked the blocking with a negative publication involving a Czech firm that had been granted a government contract.[784]

Following the release of the 'Azerbaijan Laundromat' investigation,[785] the Azerbaijani government blocked the OCCRP webpage in September 2017.[786] The article covered information on lobbying and laundering schemes of Azerbaijan authorities in the EU. Following the leak, Azerbaijani President, Ilham Aliyev, issued a statement, calling the allegations 'biased, groundless and provocative'. He stressed, 'We know that behind this are George Soros and his henchmen, who have gained a global reputation as swindlers, frauds,

[781] 'Statistika Narusheniy Prava Na Svobodu Vyrazheniya v Kazakhstane Yanvar'-Dekabr' 2017 Goda [Statistics of Violations of the Right to Freedom of Expression in Kazakhstan January-December 2017]' (21 January 2018) <http://www.adilsoz.kz/politcor/show/id/223> accessed 21 July 2019.
[782] 'V Kazakhstane Stali Massovo Blokirovat' Sayty [Kazakhstan Began Mass Blockings of Web Sites]' (*Roskomsvoboda*, 22 October 2015) <https://roskomsvoboda.org/13281/> accessed 21 July 2019.
[783] Akhal-Tech Collective (n 592).
[784] ibid.
[785] 'The Azerbaijani Laundromat' (*Organized Crime and Corruption Reporting Project (OCCRP)*, 4 September 2017) <https://www.occrp.org/en/azerbaijanilaundromat/> accessed 22 June 2019.
[786] Rowena Mason, Rajeev Syal and Luke Harding, 'Azerbaijan Hits Back over "scandalous" Money Laundering Claims' *The Guardian* (5 September 2017) <https://www.theguardian.com/world/2017/sep/05/theresa-may-challenged-over-azerbaijani-money-laundering-scheme> accessed 22 June 2019.

and liars opposed to Azerbaijan and its leadership. The dirty acts of George Soros need to be seriously investigated'.[787]

In October 2017, the district court of Kyrgyzstan ruled on blocking SoundCloud services, because the platform allegedly hosted extremist content. According to the decision, Internet users are prohibited from storing and sharing SoundCloud files, including popular music.[788]

In a comparable manner, when governments fail to restrict access to a certain service or platform, they could limit access to thousands of IP addresses. By way of illustration, in April 2015, the Security Service of Ukraine (SBU) imposed sanctions against the hosting company NIC. The provider refused to remove five webpages containing purportedly anti-Ukrainian content, and the authorities impounded hosting services from NIC's Kyiv offices. As a result, 30,000 Ukrainian websites were temporarily inaccessible.[789]

Another example is the blocking of Telegram in Russia in 2018. According to Yarovaya Law, private messenger services are obliged to provide the government with encryption keys. Telegram – the frequently used Russian messaging app – failed to comply with the requirement. Subsequently, authorities ordered the service to be blocked entirely. As of April 2018, Roskomnadzor has begun implementing the decision, causing the blocking of unrelated webpages. At a certain point, more than 18 million IP addresses were inaccessible.

---

[787] 'Soobshcheniye press-sluzhby Prezidenta [Statement from Presiden's Press Office]' (9 May 2017) <https://azertag.az/ru/xeber/Soobshchenie_press_sluzhby_Prezidenta-1090744> accessed 21 July 2019.

[788] Eldyryar Arykbaev, 'Sud v Kyrgyzstane priznal ekstremistskim muzykal'nyy servis SoundCloud [Court in Kyrgyzstan cognized SoundCloud music service as extremist]' (*KLOOP.KG*, 11 May 2018) <https://kloop.kg/blog/2018/05/11/sud-v-kyrgyzstane-priznal-ekstremistskim-muzykalnyj-servis-soundcloud/> accessed 22 June 2019.

[789] Anna Poludenko-Young, 'Ukraine's Security Service Takes Down 30,000 Websites to Fight "Pro-Russian Propaganda"' (*Global Voices*, 28 April 2015) <https://globalvoices.org/2015/04/28/ukraine-censorship-russia-propaganda-hosting/> accessed 22 June 2019.

The ban disrupted the work of banking systems, online shops, news outlets, and even other communication services such as Viber Messenger and the social network Odnoklassniki.[790]

In the preceding section, the author has already mentioned recommended principles for the states to consider when deciding to restrict online content: namely, that the ban be implemented according to the principles of legality, legitimacy, and proportionality. The issue with 'overblockings' is that the measure inevitably leads to restricting access to legitimate content online. The relevant notion may be found in the *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda,* which stipulates that:

> *state mandated blocking of entire websites, IP addresses, ports, or network protocols is an extreme measure that can only be justified if it meets the requirements of the three–part test; if there are no less intrusive alternative measures that would protect the interests; and if it respects minimum due process guarantees.*[791]

6.3. Procedures and Measures as Enshrined in Legislation and Practice: Towards Total Deanonymisation

Anonymity online falls within the ambit of two fundamental human rights: freedom of expression and the right to privacy. It implies, *inter alia*, the right of individuals to protect their private communication, digital identity, and online activities from unwanted interference. The United Nations' special rapporteur on freedom of expression, David Kaye, notes that 'encryption and anonymity are especially useful for the development and sharing of opinions, which often occur through online correspondence such as email, text messaging,

[790] 'Roskomnadzor is getting closer to breaking the Runet in pursuit of Telegram' (17 April 2018) <https://roskomsvoboda.org/38093/> accessed 22 June 2019.
[791] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda (n 665) para 1.f.

and other online interactions'.[792] The rapporteur emphasises the significant role of encryption and anonymising tools in censored environments.

However, as the author has noted in Section 4.6, national security is considered to be a legitimate reason when limiting human rights.

As to the relevant practices carried out in the post-Soviet region, it seems that regional governments join the long list of countries where anonymity is targeted by means of poorly justified restrictions.[793] These constraints take the form of VPN bans, encryption laws, mandatory registration SIM cards, and initiatives on outlawing anonymous commenting. Many of these provisions are inspired by global trends, which – when applied to post-Soviet regimes – may be pursued under the general formula of 'sharing worst practices' to extend state power.[794] Nonetheless, it is difficult to define the single centre of gravity behind the regulatory initiatives, as the regional approach shares features akin to the Chinese model (the blocking of circumvention tools), the EU model (website liability for anonymous comments), and examples from neighbouring states (notably Russia). The following sections present cases in support of the aforementioned argument.

6.3.1. VPN Blocks

Access to illegal online content may be blocked by means that have different levels of sophistication. In most cases, providers carry out the decisions of state regulators by way of IP and protocol-based blockings.[795] In this event, service providers stop relaying local IP addresses to the IPs of blacklisted web sources.

---

[792] David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye 2015 [A/HRC/29/32] para 17.
[793] ibid 36–55.
[794] Hug (n 205) 8.
[795] For a detailed explanation, see 'Technical Glossary' below.

This type of filtering is easy to bypass with circumvention tools and software, such as virtual private networks (VPNs), proxy services, and Tor anonymisers. First of all, the functionality of VPN-like services allows Internet users to access restricted content. In this case, the VPN serves as a conduit between the user's service provider and the rest of the network. The provider establishes access only between the user and the VPN – not the website the user intended to access, and the VPN's address itself is not blacklisted. Another prominent feature of these tools is the ability to ensure privacy of communication (although at various levels): VPNs hide the user's IP address and actual location, whereas Tor[796] anonymisers secure the user's identity by means of complex data encryption. Such features add complexity to the task of government agencies and service providers in monitoring a user's online activities.[797]

In the cases below, it should be noted that the official line of reasoning as regards blocking circumvention tools grossly oversimplified their functionality. Generally, lawmakers addressed the need to ensure the ban of illegal information; therefore, features *vis-à-vis* privacy of communication fell outside the scope of bills.

In Belarus, on February 2015, Resolution No. 6/8 of the Operational Analytical Centre under the President of Belarus and the Ministry of Communications and Informatisation came into force.[798] This document authorised the State Supervisory Department for Telecommunications ('BelGIE') to add circumvention and anonymising tools to the restricted access list, as they allow citizens access to blacklisted websites. The provision was formulated as follows: 'In case the State Inspectorate [State Supervisory

[796] Tor is free and open-source software designed to enable anonymous communication. It functions as a gateway between the client and the external network. It is believed that the lack of a logical connection between the sender and the message ensures reliable anonymity.
[797] Soldatov, 'The Russian VPN ban' (n 538).
[798] Ruling 'On approval of the Regulations on the procedure for restricting access to information resources (their constituent parts) on the Internet' (n 702).

Department] identified Internet resources, anonymity tools (proxy servers, Tor-like anonymous networks and others), which allow users to access Internet resources from the restricted access list, identifiers of these online resources and anonymity tools are to be added to the restricted access list'.[799]

In December 2016, Belarusian Internet users reported that the main servers of the Tor anonymisers were inaccessible.[800] Several days later, the Information Ministry confirmed that the software had been included in the Internet blacklist.[801] The officials stressed that the goal was not to block anonymous access to the Internet, but to restrict access to information forbidden by Belarusian legislation.[802]

In practice, implementation of the law was costly, time-consuming, and incapable of totally blocking all VPN-like services. In the case of Belarus, it took almost two years from the time the law entered into force until the first reported case of Tor blocking. As to the cost, in October 2015, Internet supervisor 'BelGIE' purchased an automated system to monitor anonymisation tools for BYR 878 million (approximately €387 million).[803] Even though the system did not provide for the complete blocking of circumvention services, access to them became more complicated. In December 2016, Euroradio reported that 5994 of 7010 Tor hosts were blocked in Belarus.[804] Considering that the use of circumvention tools requires

[799] Pavliuk Bykovsky, 'Belarus': blokirovka anonimayzerov v Baynete [Belarus: blocking anonymizers in Bynet]' (*DW.COM*, 25 February 2015) <https://bit.ly/2RAgFdN> accessed 24 June 2019.
[800] Pavliuk Bykovsky, 'Kak v Belarusi oboyti blokirovku Tor i izbezhat' tsenzury [How to overcome Tor blocking in Belarus and avoid censorship]' (*DW.COM*, 5 December 2016) <https://bit.ly/2FxLX0g> accessed 24 June 2019.
[801] 'Ministry of Information Admits That Tor Is Locked in Belarus' (*euroradio.fm*, 7 December 2016) <https://euroradio.fm/en/ministry-information-admits-tor-locked-belarus> accessed 24 June 2019.
[802] ibid.
[803] 'The Results of Tender Purchase No. 2015-280164-P' <http://www.icetrade.by/results/all/view/152319> accessed 24 July 2019.
[804] 'Pochti vse uzly Tor v Belarusi zablokirovany. Mogut zablokirovat' VPN i proksi? [Almost all Tor hosts in Belarus are blocked. Can VPN and proxy be banned?]' (*euroradio.fm*, 7 December 2016) <https://euroradio.fm/ru/pochti-vse-uzly-tor-v-belarusi-zablokirovanymogut-li-zablokirovat-vpn-i-proksi> accessed 24 July 2019.

some level of technical literacy, any additional obstacle to access eventually decreases the number of anonymous connections in the country.[805]

In Russia, in November 2017, *Federal Law No. 276-FZ* entered into force, requiring VPN-like providers to block access to 'blacklisted' websites.[806] According to the law, Internet regulators would demand that VPN providers connect to the 'Federal-State Information System' (FGIS) – which contains information on what web sources need to be blocked. Providers have to comply with the request within 30 days or risk being banned. From the legal perspective, there are two important consideration with respect to the bill: 1) it does not concern the overall blocking of circumvention tools, but requires providers to ensure 'blacklisted' content remains inaccessible; 2) it does not impose responsibility on ordinary users for connecting via VPNs, as regulations address VPN providers and website owners[807] (the second is similar to Belarusian law).

Further legal developments provided for administrative liability for violations of the 'Anonymiser Law'. Therefore, the Administrative Code of the Russian Federation was amended[808] in Article 19.7, which required hosting providers and 'other entities' placing circumvention services on the web to disclose information about the owners of these services. Non-compliance with the law is punishable by administrative fines: RUB 10 000-30 000 (€140-420) for private individuals, RUB 50 000-300 000 (€700-4200) for legal entities. The same package of amendments imposed fines for up to RUB 700 000 (€10 000) for search engines that refused to plug into FGIS and filter results in accordance with the state blacklist.

---

[805] ibid.
[806] Federal Law 'On Amending the Federal Law "On Information, Information Technologies and Protection of Information"'' 2017 [276-FZ].
[807] Soldatov, 'The Russian VPN ban' (n 538).
[808] Federal Law 'On Amendments to the Code of Administrative Offenses of the Russian Federation' 2018 [155-FZ].

As to the practical implementation, the 'Anonymiser Law' turned out to be virtually ineffective, and provided little leverage as regards VPN-like services.[809] Firstly, the law was contradictory to the core logic of VPNs – namely, to provide connections to censored sources. In other words, if a VPN provider started using filtration, it would lose an extensive number of clients. Most VPNs operate in foreign jurisdictions, and therefore there is no objective reason to fulfill the demands of Russian authorities. Secondly, it seems that state regulators did not have a clear idea as to how to supervise enforcement of the bill.[810]

It took almost two years from the time the bill entered into force before Roskomnadzor started issuing first notifications. On March 2019, the state regulator ordered ten popular VPN providers to apply filtering: NordVPN, Hide My Ass!, Hola VPN, Openvpn, VyprVPN, ExpressVPN, TorGuard, IPVanish, Kaspersky Secure Connection, and VPN Unlimited.[811] From all of the companies, only Russian-based Kaspersky Secure Connection complied with the demands. As a response, TorGuard removed all servers outside of Russia, since 'the legal climate in a country could pose a threat to customers' online security'.[812] At the time of reporting, July 2019, that was the single occasion when the law was applied. It should be noted that Roskomnadzor has not upheld a decision on blocking when providers refuse to connect to FGIS. In June 2019, Roskomnadzor's Head, Aleksandr Zharov, commented that the state regulator has the authority to block VPNs violating Russian

[809] Ilya Koval, 'God zakonu ob anonimayzerakh i VPN: kak im zhivetsya v Rossii? [Year to the law on anonymizers and VPN: how do they live in Russia?]' (*DW.COM*, 30 July 2018) <https://bit.ly/2M0KFfv> accessed 24 June 2019.
[810] Viacheslav Polovinko and Lilit Sarkisyan, 'Teper' oni prishli za VPN [Now they came for VPN: Roskomnadzor made the first step to "blocking ways to bypass blacklist"]' (*Novayagazeta.ru*, 28 March 2019) <https://www.novayagazeta.ru/articles/2019/03/28/80032-teper-oni-prishli-za-vpn> accessed 24 June 2019.
[811] ibid.
[812] TorGuard, 'Why TorGuard Has Removed All Russian Servers' (2018) <https://torguard.net/blog/why-torguard-has-removed-all-russian-servers/> accessed 24 June 2019.

law; however, there is no specified period for blocking. Mr Zharov suggested that administrative fines might be more effective punishment.[813]

Whereas 'Anonymiser Law' has not been used widely in the Russian Federation, on other occasions Russian authorities have relied on general anti-terrorism legislation to block circumvention tools. For instance, in May 2018, Roskomnadzor banned 50 VPN services and anonymisers that provided access to Telegram Messenger. [814] Nonetheless, state representatives did not specify the list of sources and the provisions under which the blocking was decided.

In March 2018, Kazakhstani courts ruled on blocking the IPVanish VPN service. The Kazakhstan Information Ministry requested the Yessil Court of Astana and the Auezov District Court No. 2 of Almaty to restrict access to the web source. The Ministry representative explained that the decision was linked to the fact that the VPN was used to circumvent the technical blocking of ISPs.[815]

It was not the first time users experienced difficulties with the use of circumvention tools. In June 2016, for instance, Torproject noted an interruption in the functioning of Vanilla Tor in Kazakhstan.[816]

As regards recommendations for improvement policies in analysed regions, the author suggests that the general blocking of anonymising and encryption tools should be abandoned. According to David Kaye, Special Rapporteur on the promotion and protection of the right to

---

[813] Ekaterina Bryzgalova and Kseniya Boletskaya, 'Roskomnadzor reshil poka ne blokirovat' VPN-servisy [Roskomnadzor decided not to block VPN services yet]' (*Vedomosti*, 26 June 2019) <https://www.vedomosti.ru/technology/articles/2019/06/26/805110-roskomnadzor> accessed 26 July 2019.
[814] Koval (n 809).
[815] 'Po resheniyu suda v Kazakhstane zablokirovan VPN-servis [By a court decision, a VPN service is blocked in Kazakhstan]' (*Profit.kz*, 12 March 2018) <https://profit.kz/news/45100/Po-resheniu-suda-v-Kazahstane-zablokirovan-VPN-servis/> accessed 24 June 2019.
[816] 'Censorship by Country: Kazakhstan.' (*Torproject*, 2017) <https://trac.torproject.org/projects/tor/wiki/doc/OONI/censorshipwiki/CensorshipByCountry/Kazakhstan#a20348> accessed 24 June 2019.

freedom of opinion and expression, encryption and anonymity online are essential to ensure the right of freedom of opinion and expression as well as many associated rights.[817] The Rapporteur called for the states to establish relevant national laws and to perform restrictions on a case-specific basis in accordance with the principles of legality, legitimacy, and proportionality.[818]

6.3.2. Mandatory Registration of Prepaid SIM Cards and Mobile Devices

The governments of post-Soviet countries are on a par with many other states worldwide[819] in implementing mandatory registration of prepaid SIM cards and/or mobile devices. While this measure is extremely common for national security reasons, registration has become a useful tool to maintain surveillance. This measure is especially worrisome in repressive environments (including post-Sovietstates), where anonymity is the only shield to protect vulnerable groups.[820] Registration allows authorities to access personal subscriber information, such as an home address, real name, and phone number, which enables the tracking of political opponents, journalists, and human rights defenders.

It is noteworthy that the effectiveness of SIM registration in countering crimes is dubious. Several countries that adopted this measure have faced an increasing number of identity-related crimes, along with the growth of black markets involving illegal cards and mobile devices.[821] Moreover, criminals can easily overcome mandatory registration by

---

[817] David Kaye Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (n 792) para 56.
[818] ibid 57.
[819] For instance, France, Germany, Japan, and Norway are requesting some sort of mobile user identification. Robert Stankey, Danielle Frappier and Bradley W Guyton, 'Prepaid Registration: Will US Consumers Be Required to Show Photo ID When Buying a Cell Phone?' (*Lexology*) <https://www.lexology.com/library/detail.aspx?g=16683847-6b51-4954-8a01-a2d91a3c2bde> accessed 26 June 2019.
[820] '101: SIM Card Registration' (*Privacy International*) <http://privacyinternational.org/explainer/2654/101-sim-card-registration> accessed 26 July 2019.
[821] ibid.

duplicating local SIMs, using foreign SIMs in roaming, or communicating via Internet and satellite phones.[822]

In Russia, mobile users have been obliged since 2005 to provide ID when purchasing SIM cards.[823] The mobile contract was to contain the following information: name, home address, and ID details. Nonetheless, regulations were executed on an ad hoc basis.[824] Salespersons commonly fabricated contract information, and illegally registered cards were sold everywhere on the streets. As a result, Russian lawmakers strengthened regulations on the selling of SIM cards. *Federal Law No. 304-FZ* of November 2, 2013[825] prescribed that all SIM cards should be sold in purpose-built commercial facilities, and buyers' ID details should be entered into a mobile subscription contract and sent to the operator within 10 days. In the meantime, mobile operators were required to verify the accuracy of the information involving new subscribers. The violations were punishable by administrative fines: RUB 2 000-5 000 (€30-70) for citizens, RUB 10 000-50 000 (€140-700) for state officials, and RUB 100 000-200 000 (€1 400-2 800) for legal entities. An explanatory note to the bill referred to the possibility that fake SIMs may be used in criminal activities, and '70% of all false reports about pending terrorism attacks come from mobile phones registered under falsified details'.[826]

In 2017, this law was joined by *Federal Law No. 245-FZ*, requiring mobile operators to cease communication services for subscribers who had not verified their personal

---

[822] ibid.

[823] Resolution of the Government of the Russian Federation 'On the Rules for Providing Mobile Communication Services' 2005 [328] para 18.

[824] 'Zheleznyak: Prodazha SIM-Kart v Rossii Nosit Nesistemnyy Kharakter [Zheleznyak: Saling of SIM-Cards in Russia Is Non-Systemic]' (*Edinaya Rossiya*, 22 October 2013) <http://www.er-duma.ru/press/61185/> accessed 30 July 2019.

[825] Federal Law 'On Amendments to Article 44 of the Federal Law "On Communications" and the Code of Administrative Offenses of Russian Federation' 2013 [304-FZ].

[826] Sergey Zheleznyak, Vladimir Krupennikov and Aleksey Mitrofanov, 'Document Kit to the Draft Law No. 263448-6' (19 April 2013) <https://sozd.duma.gov.ru/bill/263448-6> accessed 30 July 2019.

details.[827] Corporate clients (companies or entrepreneurs) were to indicate every employee who would use a SIM card when subscribing to communication services. The authors of the bill claimed that the use of unregistered SIMs posed a threat to the safety of citizens and the state.[828] Despite these strict provisions, some experts expressed scepticism regarding the practical execution of the law,[829] although the latest research has shown a gradual decline in the number of illegal SIMs in Russia.[830]

Likewise, users in Belarus have purchased SIM cards with ID since the early days of mobile communication. In August 2005, *Law No. 45-Z* 'On Telecommunications' entered into force, ruling that communication services are to be provided on the basis of a user-provider agreement and according to Rules for the provision of telecommunication services.[831] In line with the law, the Council of Ministers adopted the Rules in August 2006.[832] The agreement should contain the following details about subscribers: name, ID information, and place of residence.[833] Mobile subscribers should inform operators about the loss of a SIM card.[834] Under the Law on Telecommunications, operators are obliged to maintain a database of their users, containing subscribers' phone numbers, addresses, data for

[827] Federal Law 'On amendments to the Federal Law 'On Communication' 2017 [245-FZ].
[828] Valentina Matviyenko and others, 'Document Kit to the Draft Law No. 161450-7' (26 April 2017) <https://sozd.duma.gov.ru/bill/161450-7> accessed 30 July 2019.
[829] The criticism was based on several notions: firstly, it was unclear how operators would disconnect millions of 'grey' subscribers at short notice; secondly, millions of mobile users in Russia used SIMs registered to their relatives or friends; therefore, mobile operators had to carry out tens of millions of re-registrations simultaneously. *See* Mikhail Alekseyev, 'Konets Svyazi. Novyy Zakon Zastavit Operatorov Otklyuchit' Anonimnyye Sim-Karty [The End of Communication. New Bill Obliged Mobile Operators to Disconnect Anonymous SIM-Cards]' (*Forbes.ru*, 13 April 2018) <https://www.forbes.ru/tehnologii/360093-konec-svyazi-novyy-zakon-zastavit-operatorov-otklyuchit-anonimnye-sim-karty> accessed 30 July 2019.
[830] Denis Kuskov, CEO of the analytics agency Telecom Daily, commented that the number of illegal SIM cards in 2018 had declined by 15-17% comparing to the previous year. See Alena Suharevskaya, 'Eksperty otsenili kolichestvo serykh sim-kart v Rossii [Experts estimated illegal SIMs in Russia]' (*Vedomosti*, 5 July 2019) <https://www.vedomosti.ru/technology/articles/2019/07/05/805917-eksperti-otsenili> accessed 30 July 2019.
[831] The Law 'On Telecommunications' 2005 [45-Z] Art. 56.
[832] Resolution of the Council of Ministers of the Republic of Belarus 'On Approving the Rules for the Provision of Telecommunication Services' 2006 [1055].
[833] Details on the agreement with mobile operators were specified in 2009, under Resolution of the Council of Ministers of the Republic of Belarus 'On amendments and addenda to the Resolution from 17 August, 2006 No. 1055' 2009 [677] para 76.
[834] ibid 187.

the identification of subscribers or their communication devices, and requisites of a user's official state ID.[835] Since 2016, Belarusian operators of electronic communication have signed agreements with new users only after the user's ID has been checked with the Ministry of the Interior's database.[836] Called 'Passport', the base is helping operators to check the validity of the documents. Yet another new provision enacted in 2016 requires a photo or a video of the new subscriber to be saved and kept.[837]

In Uzbekistan, rules for the provision of mobile services were introduced in 2009.[838] Similar to Belarusian and Russian legislation, regulations have prescribed that mobile services be carried out according to the operator-subscriber contact. The contract should include name, home address, and ID details of the new subscriber. Users are required to notify the operator in the event that the SIM card was lost, otherwise they could be charged for mobile services obtained with the lost card.

Since February 2014,[839] Kyrgyzstan SIM cards may be purchased only after registration, whereas former regulations required registration within one year. The agreement for communication services should include the subscriber's name and ID details. In its latest reports, Freedom House has expressed the concern that mandatory registration may result in complications for users with regard to enjoying anonymous communication.[840]

---

[835] The Law 'On Telecommunications' (n 831) Art. 56.

[836] Resolution of the Ministry of Internal Affairs of the Republic of Belarus, Operational Analytical Center under the President of the Republic of Belarus and the Ministry of Communication and Informatization of the Republic of Belarus 'On the procedure for the confirmation of telecommunications operators information about the subscriber' 2016 [211/11/9].

[837] Resolution of Operational Analytical Center under the President of the Republic of Belarus 'On the system of countering violations of traffic transmission on telecommunication networks' 2016 [55] ch 2 para 11.

[838] Order of the General Director of the Uzbek Agency of Communication and Informatization 'On the Approval of the Rules for the Provision of Mobile Communication Services' 2009 [1990-son].

[839] Decree of the Government of the Kyrgyz Republic 'On the Regulations on mobile radio telephone service' 2014 [97].

[840] 'Freedom on the Net 2018: Kyrgyzstan' (n 543).

In Kazakhstan, the mobile service agreement includes information on the user's postal address, e-mail, and ID information.[841] Communication services are provided based on the agreement, likewise in the cases below.

Apart from the registration of SIM cards, several countries under scrutiny require the registration of mobile devices to create databases of IMEI codes – international 15-digit serial numbers of each mobile device, which allow geo-tracking of the same device. In short, IMEI (International Mobile Equipment Identity) facilitates the recognition of stolen or lost phones. When a user makes a call, the operator determines the IMEI code and the location of the device, so it is possible to track the phone via IMEI.[842] Knowing that the device has fallen into the wrong hands, the operator can block stolen equipment from using the communication services. Although IMEI registration has proven to be an effective tool in preventing mobile theft, it could be argued that in the countries under scrutiny such measures can seriously challenge the anonymity of mobile users, given that telecommunication providers are generally obligated to cooperate with intelligence services,[843] and the environment for human rights in the region is considered to be poor.[844]

In Azerbaijan, on 28 December 2011, Azerbaijan's Cabinet of Ministers approved the *Decision No.212* on 'Rules of Mobile Devices Registration'. According to the new provisions, each mobile device imported to Azerbaijan for private use should be registered within 30 days (with an SIM card from the country's mobile operators).[845] The application

---

[841] 'Terms of Mobile Services (Annex)' (24 February 2015) para 1 <//online.zakon.kz/Document/?doc_id=33812603> accessed 26 June 2019.

[842] Miguel Leiva-Gomez, 'Everything You Should Know About Your IMEI Number' (*Make Tech Easier*, 6 August 2018) <https://www.maketecheasier.com/imei-number/> accessed 31 July 2019; 'The Many Identifiers in Our Pockets: A Primer on Mobile Privacy and Security' (*The Citizen Lab*, 21 May 2015) <https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/> accessed 31 July 2019.

[843] See Section 6.3.5, *'Requirements for operators to store data and provide access to authorities'*.

[844] Hug (n 205).

[845] 'Mobile Devices Registration System' (*Ministry of Transport, Communications and High Technologies*) <https://rabita.az/en/c-projects/mdrsen/> accessed 26 June 2019.

required information on official state ID, IMEI code, and mobile phone number. Unregistered equipment was listed on a 'black page' and disconnected from mobile services. The new requirements came into force in the spring of 2013.[846]

In Kazakhstan, the provision requiring Kazakh users to register mobile phones in the IMEI database came into force in July 2017.[847] Notably, Kazakhstan lawmakers introduced the development in a counter-terrorism package, whereas neighbouring countries (Uzbekistan, Azerbaijan) argued the need for enforcing registration as a measure to combat mobile theft and smuggling. As the next step, users were obliged to link their registered devices with governmental IDs and phone numbers.[848] Therefore, the Information and Communication Ministry was able to identify phone owners by their IMEI number.

In Uzbekistan, the mobile registration system was enacted under *Ruling of Cabinet of Ministers No. 847-son* from 22 October 2018.[849] The system was launched on 1 April 2019. A representative of the Ministry for Communication and Information Technology Development (the state-authorised body) stressed that providers would register their subscribers automatically, and therefore the process did not require any action on the part of users.[850]

---

[846] 'IMEI –Codes Registration System to Be Applied in Azerbaijan' (*News.Az*, 15 March 2013) <https://news.az/articles/tech/77977> accessed 26 June 2019.

[847] Law of the Republic of Kazakhstan 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Countering Extremism and Terrorism' (as amended on February 27, 2017) (n 721); 'Kazakhstan: S 1 iyulya 2017 goda operatory budut blokirovat' nezaregistrirovannyye telefony [Kazakhstan: From July 1, 2017, operators will block unregistered phones]' (*Digital Report*, 25 January 2017) <https://digital.report/kazahstan-s-1-iyulya-2017-goda-operatoryi-budut-blokirovat-nezaregistrirovannyie-telefonyi/> accessed 27 June 2019.

[848] Zhadra Zhulmukhametova, 'Privyazyvat' Nomera Telefonov Abonentov k IIN Nachnut Uzhe Letom 2018 Goda [Binding the Phone Numbers of Subscribers to the Identification Numbers Will Begin in the Summer of 2018]' (16 May 2018) <https://informburo.kz/novosti/privyazyvat-nomera-telefonov-abonentov-k-iin-nachnut-uzhe-letom-2018-goda.html> accessed 27 June 2019.

[849] Ruling of Cabinet of Ministers of the Republic of Uzbekistan 'On measures to streamline the system of accounting for mobile devices in the Republic of Uzbekistan' 2018 [847-son].

[850] Temir Isayev, 'V Uzbekistane registratsiya mobil'nykh telefonov po IMEI budet besplatnoy [IMEI Registration of Mobile Devices will be Free of Charge in Uzbekistan]' (*Podrobno.uz*, 30 March 2019) <https://podrobno.uz:443/cat/tehnp/v-uzbekistane-registratsiya-/> accessed 1 August 2019.

Considering that the mandatory registration of pre-paid SIM cards is a common practice in many states worldwide, the author is hesitant to recommend that the countries under scrutiny abandon such a requirement. However, the revision of existing approaches might provide for better protection of citizens' anonymity and related human rights. The identification of users, in particular through SIM card registration, should not be a condition for access to digital communications.[851]

6.3.3. Other Means of Pre-Emptive Deanonymisation

In Russia, the requirement to identify users of messengers and social media was introduced under *Federal Law No. 241-FZ* from 29 July 2017.[852] New provisions required messaging and social media platforms to link user accounts with mobile numbers, under an 'identification contract' between a messenger service and a communication service provider. The law entered into force on 1 January 2018, but it took another year before it was fully implemented. The substantive sub-decree, *Government Resolution No. 1279 'On Rules for Internet Users Identification by Instant Messaging Services'*, became effective only in May 2019.[853] The identification procedure was established as follows: 1) when registering a new subscriber, the messenger service should identify the owner of the phone number via a request to the mobile service provider; 2) a service provider must reply within 20 minutes; 3) in the event that identification is successful, a service provider must update its database with the user's unique ID on a messenger platform and indicate the fact of registration; 4) in the event that verification fails, a messenger service must deny services for such a user.[854]

---

[851] David Kaye Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (n 792) para 60.

[852] Federal Law 'On Amending Articles 10.1 and 15.4 of the Federal Law 'On Information, Information Technologies and Protection of Information' 2017 [241-FZ].

[853] Resolution of the Government of Russian Federation 'On Rules for Internet Users Identification by Instant Messaging Services' 2018 [1279].

[854] 'The government has banned registration in instant messengers by other people's numbers' (*Habr*, 6 November 2018) <https://habr.com/ru/news/t/428874/> accessed 1 August 2019.

Commenting on the Resolution, Roskomnadzor's Head, Aleksandr Zharov, stressed that anonymous communication via messengers brought complexities to law enforcement operations and the investigation of crime, and therefore identification was a necessary step to ensure a safe communication environment.[855]

It should be noted that ordinary users, in principle, are not prosecuted for lack of registration. For instance, a violation of the above rules by a messaging service is punishable by administrative fines: RUB 3 000-5 000 (€40-70) for citizens, RUB 30 000-50 000 (€420-700) for state officials, and RUB 800 000-1 000 000 (€11 200-14 000) for legal entities.[856] Moreover, a messenger service may be banned for non-compliance under Article 15.4 of the *Law 'On Information, Information Technologies and Protection of Information'*.

In Kazakhstan, Internet users have recently been banned from posting anonymous comments on local websites. This provision was enforced under a set of amendments to legislative acts in communication, approved by President Nazarbayev in December 2017.[857] To leave a comment, users are required to sign an electronic agreement with the website, and to identify themselves via an electronic seal or by sending a short text message to obtain a password. The law allows user pseudonyms, although it does not change the fact that authorities can easily identify online commentators, as the latter still provide real-world details to the website.

Dauren Abayev, Minister of Information and Communications, justified new regulatory norms with the need to eliminate hate speech and social and ethnic hatred online: 'In the case of inciting hatred, calls for unconstitutional actions, I think there will be an

[855] ibid.
[856] Federal Law 'On Amendments to the Code of Administrative Offenses of the Russian Federation' 2017 [396-FZ].
[857] The Law 'On Changes and Addenda to Some Legislative Acts of the Republic of Kazakhstan on Information and Communications' 2017 [128–VI].

opportunity to track [the authors], and law enforcement agencies will have the opportunity to respond'.[858]

When the rule entered into force in January 2018, the Information Ministry assured it would not demand immediate compliance from website owners. Therefore, local web sources were given an extension until the end of March to establish identification mechanisms. Thereafter, websites could face fines starting from €700.[859]

The Republic of Belarus enacted the mandatory identification of online commentators from 1 December 2018, among other restrictive provisions of amended Media Law. In particular, new regulations required website owners to 'prevent posting […] of informational messages and (or) materials (including commenting) by other users without their prior identification'.[860] In November 2018, the Council of Ministers introduced a decree in line with the amendments, clarifying the user identification procedure.[861] Under the established order, prior to posting on web sources, users should register via SMS or 'with any other details confirming their identity'.[862] The terms and conditions should inform the user regarding the inadmissibility of publications violating Belarus law.

The collected data was required to be stored on Belarusian servers for the duration of the user agreement, as well as for a year from the date of its termination.

Harlem Désir, OSCE Representative on Freedom of the Media, stressed that, 'Many of the provisions [of the law] are excessive and disproportionate and could result in the

[858] 'Nazarbayev zapretil anonimnyye kommentarii v internete [Nazarbayev Banned Anonymous Comment Online]' (*NUR.KZ*, 28 December 2017) <https://www.nur.kz/1710097-nazarbaev-zapretil-anonimnye-kommentarii-v-internete.html?> accessed 1 August 2019.
[859] Almaz Kumenov, 'Kazakhstan: Online Anonymity Ban in Force from April' (*Eurasianet*, 2 February 2018) <https://eurasianet.org/kazakhstan-online-anonymity-ban-in-force-from-april> accessed 27 June 2019.
[860] Law 'On making changes and additions to some laws of the Republic of Belarus' (n 657).
[861] Decree of the Council of Ministers of the Republic of Belarus 'On the procedure for preliminary identification of users of the Internet resource, online media' 2018 [850].
[862] 'Opredelen Poryadok Predvaritel'noy Identifikatsii Pol'zovateley Internet-Resursa [The Procedure for Preliminary Identification of Users of the Internet Resource]' (*Pravo.by*, 26 November 2018) <http://www.pravo.by/novosti/novosti-pravo-by/2018/november/31459/> accessed 27 June 2019.

curtailing of freedom of expression, including the right of citizens to remain anonymous online'.[863]

Limiting anonymous commenting is not the only measure targeting online anonymity in the states analysed. Another popular initiative 'travelling' throughout these states is related to controlling payments online. While anonymous online payments might be misused to finance terrorism,[864] it is equally true that a significant number of independent media worldwide are financed by readers' donations.[865] Therefore, the initiatives in regulating online payments indirectly concern freedom of expression.

In Belarus, under *Ordinance No. 6 of 28 December 2014 'Concerning prompt measures to counteract the illegal drug trade'*, online payment systems such as PayPal and Webmoney may not be used anonymously. Private individuals shall be identified when opening 'web wallets', irrespective of the amount of currency they plan to store online.[866] According to the official statement on the President's website, the measure is justified by the need to prevent drug abuse and 'to protect the health and lives of Belarusian citizens'.[867]

In Kazakhstan, the possibility of prohibiting anonymous online payments was discussed in September 2016. Kalmukhanbet Kasymov, the Minister of the Interior, suggested that the measure could be effective in combating drug trafficking.[868]

---

[863] Harlem Désir, 'Legislative Amendments Further Restrict Media in Belarus, Says OSCE Media Freedom Representative' (*OSCE*) <https://www.osce.org/representative-on-freedom-of-media/384786> accessed 27 June 2019.
[864] United Nations Office on Drugs and Crime (n 438).
[865] Bibi van der Zee, 'How Reader Funding Is Helping Save Independent Media across the World' *The Guardian* (25 December 2017) <https://www.theguardian.com/technology/2017/dec/25/how-reader-funding-is-helping-save-independent-media-across-the-world> accessed 2 August 2019.
[866] Ordinance 'Concerning prompt measures to counteract illegal drug trade' 2014 [No. 6].
[867] 'Freedom on the Net 2015: Belarus' (n 687).
[868] Meyirim Smayil, 'Zapretit' anonimnyye onlayn-platezhi namereny v Kazakhstane [Kazakhstan plans to prohibit anonymous online payments]' (*Tengrinews.kz*, 26 September 2018) <https://tengrinews.kz/kazakhstan_news/zapretit-anonimnyie-onlayn-plateji-namerenyi-v-kazahstane-354366/> accessed 2 August 2019.

On 26 July 2019, the Russian Federation Council approved amendments to the *Federal Law 'On the National Payment System' and the Federal Law 'On the Central Bank of the Russian Federation'*, and sent them for signing by the President.[869] The amendments prohibit the replenishing of anonymous online wallets from the terminals and offices of mobile providers. The owners must use their local bank account and provide documents. Anatoly Aksakov, a member of the Russian State Duma and co-author of the draft bill, said that the amendments had been proposed to reduce financing of the drug trade and terrorism.[870]

In the above sections, the author has covered several recommendations regarding anonymity and encryption in the digital age, which are relevant for this section as well: in particular, restrictions should be founded on the principles of legality, legitimacy, and proportionality, and states should avoid any unnecessary identification of users in relation to digital access. Moreover, the relevant notions could be drawn from the following general principles declared by Amnesty International:[871]

- When imposing restrictions regarding anonymity and encryption, states should provide for 'detailed and evidence-based justification';
- States should ensure the implementation of precise and transparent laws when interfering with the use of encryption;
- The requirement to provide encryption keys should be a subject of judicial approval;

[869] 'Draft Bill No. 603170-7 'On Amending to the Federal Law "On National Payment System" and the Federal Law "On the Central Bank of the Russian Federation"' (*Duma.gov.ru*) <https://sozd.duma.gov.ru/bill/603170-7> accessed 2 August 2019.
[870] 'Senatory zapretili popolnyat' anonimnyye elektronnyye koshel'ki cherez terminaly [Senators banned replenishing anonymous electronic wallets via terminals]' (*Novayagazeta.ru*, 29 July 2019) <https://www.novayagazeta.ru/news/2019/07/29/153746-senatory-zapretili-popolnyat-anonimnye-elektronnye-koshelki-cherez-terminaly> accessed 2 August 2019.
[871] 'Encryption: A Matter of Human Rights' (Amnesty International 2016) POL 40/3682/2016 36–37.

- Measures should be applied narrowly, only when necessary, and be proportionate to the legitimate aim;

- States should take the least intrusive approach to achieve the desired goal when preventing encryption;

- States should avoid applying restrictions that would be discriminatory with respect to certain social groups;

- Restrictive measures should be challenged and overseen by an independent authority.

6.3.4. Third-Party Liability

In recent years, there has been an increasing trend in international legal practice to impose responsibility for online content regulation on the private sector,[872] including moderating anonymous user comments. Such an approach is by no means geographically limited, and it encompasses a number of states across the European Union as well the USA,[873] which were taken as a benchmark in the present study.[874] Nonetheless, to date there are no clear answers in jurisprudence and the practical application of the law – cases like *Delfi AS v Estonia* and *MTE v Hungary* send conflicting signals (see above in Section 5, *Expression Online: Best Practices and Existing Frameworks in the 'Old' Democracies*).

The practice of intermediary liability online raises several concerns with respect to freedom of expression. Firstly, being responsible for offensive user content, the owners of online platforms are turning into censors and forced to tackle legitimate online expression. As private actors, they may establish moderating mechanisms having poor transparency, or

[872] Muižnieks (n 490).
[873] Adam Holland, Chris Bavitz and Jeff Hermes, *Intermediary Liability in the United States* (Global Network of Interdisciplinary Internet & Society Research Centers (NoC) 2015).
[874] In Section 5, '*Expression Online: Best Practices and Existing Frameworks in the 'Old' Democracies*, the author describes an approach by the ECtHR in adjudicating the issue of intermediary liability for regulation of the online environment, particularly in the cases *Delfi AS v Estonia* and *MTE v Hungary*.

affecting the user's ability to appeal against the ban.[875] Secondly, this trend is intertwined with pre-emptive deanonymisation techniques, as it incentivises online platforms to prohibit anonymous/pseudonymous speech.[876]

Within the analysed regions, legal grounds for imposing liability on web sources are established not only through selected court cases but also by means of specific regulatory laws in the online sphere.

As early as 2009, the Supreme Court Plenary of Ukraine ruled that if the author of defamatory online content is unknown or anonymous, the responsibility falls on the website owners, as they created the technical capabilities with regard to disinformation.[877] Noteworthy is that the Resolution of the Supreme Court Plenary is not a normative legal document, and the provisions enshrined in the Resolution are not generally binding. This fact generates a great deal of controversy in any decision as to whether a website owner should be held liable when defamatory information is posted online anonymously.[878] However, up to the present time no specific law regarding the issue has been adopted.

In 2010, The Supreme Court of the Russian Federation adopted a ruling[879] clarifying the responsibilities of website owners. The Court stated that Internet media may not be held responsible for comments, equating them to copyrighted works broadcast without prior recording (in the same way that editors of a TV programme are exempted from liability involving information broadcast live). However, in order to be released from liability, user

---

[875] 'Internet Intermediaries: Dilemma of Liability' (*Article 19*, 20 August 2013) <https://www.article19.org/resources/internet-intermediaries-dilemma-liability/> accessed 3 September 2019.

[876] David Kaye Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (n 792) para 54.

[877] *On the case law on the protection of the dignity and honor of the individual, as well as the business reputation of the individual and the legal entity* [2009] the Supreme Court Plenary of Ukraine 1.

[878] Tetyana Startseva, 'Shchodo Vidpovidal′nosti Vlasnyka Veb-Sayta [On the Responsibility of Website Owners]' (*Liga*, 13 October 2013) <https://blog.liga.net/user/tstartseva/article/12481> accessed 3 September 2019.

[879] *On the Application of the Law of the Russian Federation 'On Mass Media' by the Courts* [2010] The Supreme Court Plenary of the Russian Federation 16.

comments must be posted without prior moderation or editing. Only in this case can the editors not be held responsible for the actions of third parties. If the comment is published after a preliminary check by an employee of the site, both the user and the media site editorial staff can be held liable for distributing the comment in question.

In Armenia, Members of Parliament proposed regulations on defamatory online comments in March 2014. If it had been passed, Amendments to Article 1087.1 of the Civil Code would have imposed liability for online media that contained offensive comments from anonymous and fake users. The web platforms would have been required to delete the libellous comment within 12 hours unless they identified the author.[880] The MPs explained the initiative in terms of the growing issue of defamation under fake social media accounts and the need to determine who is legally responsible in these cases. The draft law raised serious concerns with respect to freedom of expression, largely owing to vague definitions and a lack of clarity.[881] The proposed legislation resulted in a public outcry, and has therefore been shelved indefinitely.[882]

Among other provisions targeting online expression, the Amendments to Belarusian Media Law from 2014 rendered websites responsible for user-generated content. The owners of Internet sources must not allow the dissemination of information that contradicts the Law.[883]

---

[880] Kimberly Carlson, 'Armenian Bill Threatens Online Anonymity' (*Electronic Frontier Foundation*, 16 April 2014) <https://www.eff.org/deeplinks/2014/04/armenian-bill-threatens-online-anonymity> accessed 6 July 2019.

[881] Oreste Pollicino, 'Legal Analysia of Draft Amendments to the Civil Code of the Republic of Armenia' (Office of the OSCE Representative on Freedom of the Media 2014) <https://www.osce.org/fom/116911?download=true> accessed 7 June 2019.

[882] 'Expert: The Year Was Rather Tense for Armenian Jouranalists' (*yerkramas.org*, 19 December 2014) <http://yerkramas.org/article/85307/uxodyashhij-god-byl-dlya-armyanskix-zhurnalistov-dostatochno-napryazhennym-%E2%80%93-ekspert> accessed 2 August 2019; 'Komissiya Parlamenta Armenii Reshila «otlozhit' v Dolgiy Yashchik» Skandal'nyy Zakonoproyekt Protiv «feykov» [The Parliamentary Commission Indefinetely Posponed Unfamous Fake News Bill]' (*Panorama.am*, 25 April 2014) <https://www.panorama.am/ru/news/2014/04/25/a-bill-about-press/301560> accessed 2 August 2019.

[883] Bastunets (n 555).

As a result, moderators of Belarusian online forums were forced to apply tough self–censorship.[884] The legislative amendments of 2018 imposed an even broader list of responsibilities[885] on website owners; in particular, they are required:

- to analyse the content of the Internet resource;
- not to allow the dissemination of information that is prohibited by the Law and other legislative acts of the Republic of Belarus, or materials containing obscene words and phrases;
- not to allow the dissemination of unreliable information that may harm state or public interests;
- not to allow the dissemination of false information that discredits the honour, dignity, or business reputation of individuals or the business reputation of legal entities.

An amended Criminal Code of the Republic of Kazakhstan from July 2014 contains provisions that impose responsibility on social media users to moderate comments in their personal accounts. The Committee on Communication, Informatisation, and Information clarified that users may be held responsible under Article 183, 'allowing publication of extremist materials on mass media'. According to the regulator, extremist comments from unrelated users may lead to a maximum sanction of 90 days imprisonment. Dissemination of illegal content – even reposted – on certain occasions entails a 20-year prison sentence.[886]

---

[884] Alexandr Nikolaichuk, 'Moderatory na forumakh v Belarusi vypolnyayut rol' vakhterov i okhrannikov [Moderators on Belarus forums take the role of watchmen and security guards]' (*Digital Report*, 27 January 2017) <https://digital.report/moderatoryi-na-forumah-v-belarusi-vyipolnyayut-rol-vahterov-i-ohrannikov/> accessed 6 July 2019.

[885] Law 'On making changes and additions to some laws of the Republic of Belarus' (n 657) Art 30.1.

[886] Alisher Ahmetov, 'Kazakhstantsev mogut arestovat' za chuzhiye kommentarii na ikh stranitsakh v sotssetyakh [Kazakhstanis can be arrested for the comments of others on their pages in social networks]' (*Tengrinews.kz*, 21 October 2015) <https://tengrinews.kz/kazakhstan_news/kazahstantsev-mogut-arestovat-chujie-kommentarii-ih-282818/> accessed 7 July 2019.

The relevant recommendations for the states with regard to the issue may be found in the *Manila Principles on Intermediary Liability*. In this document, the coalition of civil society organisations called for governments:[887]

- to provide accessible legislation regarding intermediary responsibilities; third parties should not be held liable if they are not involved in editing user content;
- orders to take down the content should be a matter of judicial supervision;
- a request to take down content should be clear, unambiguous, and contain a clear legal basis for the restriction;
- respective laws should be drafted in accordance with the principles of necessity and proportionality;
- aside from exceptional circumstances, intermediaries and users should be guaranteed the right to appeal the ban decision;
- governments should follow the principles of transparency and accountability; therefore, the respective regulations, restrictive orders, and court decisions should be accessible.

6.3.5. Requirements for Providers to Store Data and Provide Access to Authorities

Another step towards the deanonymisation of Internet users, taken by many of the governments analysed, lies in the requirement for ISPs to identify customers, to store the data about online activities, and to provide it at the request of the authorities. It should be noted that the development is not new in international practice. In the EU, mandatory data retention was introduced following the 9/11 terrorist attacks,[888] and to date it remains in the legislation

[887] 'Manila Principles on Intermediary Liability' (A Global Civil Society Initiative 2015).
[888] Abu Bakar Munir and others, 'Data Retention Rules: A Dead End' (2017) 3 Eur. Data Prot. L. Rev. 71.

of many member states.[889] However, because the European Court of Justice ruled that blanket data retention was invalid in EU law,[890] several countries revised theirs.[891]

As for data retention in the former Soviet region, it seems that such a regulation adds to the list of examples where regional governments drew inspiration from the 'worst practices'[892] of old democracies.

By way of illustration, Presidential Decree No. 60, adopted in Belarus in 2010, required stricter regulations over the Internet sphere. The stated aim of the decree was to protect the interests of citizens, society, and the state in the area of information, and to provide for the development of a national segment of the Internet.[893]Amendments obliged the owners of Internet cafés to identify their clients, and to store records on their personal data and provided services for one year. In turn, Internet providers were required to identify subscriber sets used for rendering the Internet services, and to keep this information for one year. Government bodies – investigative authorities, courts, Public Prosecutor office, and so on − were authorised to request data at any time.[894]

In Georgia, until more recently, State Security Services were granted direct access to users' online communication.[895] However, the Constitutional Court overruled this practice in 2016, as it violated the privacy of Georgian citizens'.[896]

---

[889] 'Data Retention across the EU' (*European Union Agency for Fundamental Rights*, 16 December 2015) <https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention> accessed 17 September 2019.

[890] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (n 513).

[891] Munir and others (n 888). The national laws were revised, inter alia, in Slovakia and Luxemburg, see 'Data Retention across the EU' (n 889).

[892] Hug (n 205).

[893] 'The Decree of the President of the Republic of Belarus No. 60 "On the Issues to Improve Making Use of the National Segment of Internet" (Unofficial Translation)' (*E-Belarus.ORG*) <http://www.e-belarus.org/docs/decree60.html> accessed 2 July 2019.

[894] ibid.

[895] Tamar Chkheidze, 'Internet Control in Georgia' (*HUMANRIGHTS.GE*, 17 November 2010) <http://www.humanrights.ge/index.php?a=main&pid=12564&lang=eng> accessed 2 July 2019.

Kazakh ISPs were required to keep user data[897] for two years, according to a decree from December 2011. The Prosecutor General's Office may request such information for operative-investigatory bodies, including the National Security Committee or intelligence agencies. Cyber cafés were obliged to retain users' browsing history and online activities for a minimum of six months.[898]

In March 2014, Uzbek authorities updated requirements for Internet cafes and public access points. Thus, operators were to install surveillance cameras and store users' log files for three months.[899]

In 2015, Azerbaijani lawmakers updated the Law on Operative-Investigative Activity. Law enforcement agencies were empowered to organise surveillance without judicial approval,[900] with a view to ensuring national security and preventing crime.[901]

In Russia, the most egregious provisions of the 2016 Russian Yarovaya Law[902] seem to be imposed *vis-à-vis* private communication. The new regulations require messenger

---

[896] 'Freedom on the Net 2016: Georgia' (n 583).

[897] Kazakh legislation established a special category of information to be stored for investigative purposes: namely, 'user service information', which includes information on subscriber numbers, IMEI codes of devices, billing details, IP addresses, browsing history, and data transmission protocols. The current regulations are established under the Order of the Acting Minister for Investment and Development of the Republic of Kazakhstan, appendix 3 'Rules for the provision of Internet access services' (as amended on 28 May, 2018) 2015 [171]; Decree of the Government of the Republic of Kazakhstan 'On approval of the Rules for communication operators for collection and storage of user service information' (as amended on 28 April, 2018) 2010 [246].

[898] Rules for the provision of Internet access services 2011 [1718].

[899] Resolution of the State Committee for Communications, Informatization and Telecommunication Technologies of the Republic of Uzbekistan 'On introducing changes and additions to the Regulation on the procedure for providing access to the Internet in public facilities' 2014 [79–mx].

[900] Law of the Republic of Azerbaijan on operational investigative activities 1999 [728-IQ] Art 10, Section IV.

[901] *Decision on interpretation of some provisions of the Articles 137 and 4452 of the Criminal Procedure Code of the Republic of Azerbaijan* [2015] Plenum of Constitutional Court of the Republic of Azerbaijan AZE-1999-1-003.

[902] 'Yarovaya Law' – an antiterrorist legislative package that contains some of the harshest rulings in post-Soviet Russia. They affected nearly a dozen laws, with serious consequences for freedom of the Internet. The set is based on the Federal Law 'On Amendments to the Federal Law "On Counter-Terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety' 2016 [374-FZ]; Federal Law 'On Amendments to the Criminal Code of the

services and social networks[903] to: 1) keep communication logs and users' personal data for a year[904] and 2) provide them on demand to law enforcement agencies along with encryption keys. All information must be stored within Russia, and information companies the risk of being banned for non-compliance. Senior HRW Internet researcher, Cynthia Wong, said after the amendments that, 'No digital communication would be safe from government snooping, no matter how innocuous or unrelated to terrorism'.[905]

In short, the legislation creates a precedent for the storage of personal data on a previously unseen scale, and makes criminally punishable the expression of a wider range of opinions on the Internet, further eroding online freedom of expression in Russia. The approach to data retention taken by the Russian legislature is in stark contrast to the position recently expressed by the ECJ, as described above. The laws under scrutiny have been criticised not only by journalists and human rights advocates[906] but also by some Russian state-funded experts.[907] Firstly, the legislation creates, on a previously unseen scale, a precedent for the storage of personal data, making any security breaches a non-trivial event from the perspective of data protection.[908] Secondly, the representative of the biggest[909]

Russian Federation and the Criminal Procedure Code of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety' 2016 [375-FZ].

[903] The regulations are imposed on 'information distributors' – Internet services listed in Roskomnadzor's registry. For instance, Facebook, WhatsApp, Instagram are not included in the list. See 'Internet Distributor Registery' (*Roskomnadzor*) <https://97-fz.rkn.gov.ru/> accessed 28 June 2019; 'Registery of Information Distributors' (*Roskomsvoboda*) <https://reestr.rublacklist.net/distributors_main/> accessed 28 June 2019.

[904] Communication operators are required to store metadata for three years.

[905] 'Russia: "Big Brother" Law Harms Security, Rights' (*Human Rights Watch*, 12 July 2016) <https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights> accessed 28 June 2019.

[906] Ronald Bailey, 'I Learned It By Watching You!' (2016) 48 Reason 18–19 <https://reason.com/2016/11/01/i-learned-it-by-watching-you/> accessed 4 October 2019.

[907] 'Zakonoproyekty Ozerova i Yarovoy Ne Snizyat Terroristicheskoy i Ekstremistskoy Ugrozy i Nuzhdayutsya v Pererabotke [Bills by Ozerov and Yarovaya Will Not Reduce the Terrorist and Extremist Threats and Need to Be Improved]' (*Council under the President of the Russian Federation on the development of civil society and human rights*, 2016) <http://president-sovet.ru/presscenter/news/read/3151/> accessed 20 September 2019.

[908] Sergey Potresov, '«Popravki Yarovoy i Ozerova», Tsena Voprosa [Amendments by Yarovaya and Ozerov: The Price]' (2016) <https://mobile-review.com/articles/2016/data-storage.shtml> accessed 20 September 2019.

[909] Victor Savitsky, 'Kvartal'nyy podschet [Quarterly count]' (*Comnews*, 2016) <http://www.comnews.ru/content/103556/2016-09-01/kvartalnyy-podschet> accessed 20 September 2019.

Russian telecom operator, MTS, pointed out that − given MTS's current income figures − they will have to put all of their profits into the data centre infrastructure for the next 100 years to fully implement data storage provisions and ensure compliance with Yarovaya's Laws.[910] The fact that most Russian telecoms will not be able to comply with this legislation may actually be to the government's advantage; those companies will become *de facto* criminals, giving state authorities 'the leverage to extract from them any other concession it desires'.[911]

In April 2018, the popular messaging platform, Telegram, refused to provide encryption keys to the Federal Security Service (FSB).[912] Consequently, a Moscow court ordered the app to be banned. The blocking affected nearly 16 million unrelated IPs, used by Google Cloud and Amazon's Web Services.[913]

Since January 2016, Internet providers in Belarus have been required to keep records of users' browsing history. The information must be stored for one year, and law enforcement agencies are granted access.[914]

Article 637 of Kazakhstan's Administrative Code imposes fines on providers up to a maximum of KZT 505 000 (€1 200) for providing access to banned information.[915] Article 637.3 of Kazakhstan's Administrative Code imposes fines up to a maximum of KZT 1,3 million (€3 050) for violating the obligation to collect and store subscribers' service information. In April 2018, the government amended the rules for operators on the storage of

[910] Potresov (n 908).
[911] Bailey (n 906).
[912] Andrew Roth, 'Moscow Court Bans Telegram Messaging App' *The Guardian* (13 April 2018) <https://www.theguardian.com/world/2018/apr/13/moscow-court-bans-telegram-messaging-app> accessed 27 June 2019.
[913] Andrew Roth, 'Russia Blocks Millions of IP Addresses in Battle against Telegram App' *The Guardian* (17 April 2018) <https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app> accessed 27 June 2019.
[914] 'Freedom on the Net 2015: Belarus' (n 687).
[915] Code of the Republic of Kazakhstan on Administrative Offenses 2014 [235–V].

user data.[916] The new provision requires the storage of information on subscribers in the territory of Kazakhstan. Mobile operators and ISPs collect the following information: phone numbers, postal address, billing information, taxpayer identification number, IP address, network protocols, URL history, and so forth.[917]

As a way to improve existing state policies, the author refers in this section to the recommendations suggested by David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, which are described in detail in the sections below. In particular, the Rapporteur noted that 'emergency situations do not relieve States of the obligation to ensure respect for international human rights law', warning that the states should avoid concentrating solely on crime-prevention aspects when dealing with encryption and anonymity.[918]

6.4. Procedures and Measures as Enshrined in Legislation and Practice: Mass Surveillance

6.4.1. SORM

The evidence of cross-fertilisation in online regulation across the post-Soviet region is particularly apparent on the technological side, in the form of establishing the same surveillance systems. In this regard, the countries under scrutiny are copying the Russian framework of 'lawful interception' and surveillance.

Cooperation between private technology companies in Russia, the Russian Federal Security Service (the FSB), and security agencies in neighbouring countries may be

[916] On Amendments and Additions to the Resolution of the Government of the Republic of Kazakhstan from March 30, 2010 No. 246 'On Approval of the Rules for Telecommunications Operators to Collect and Store Service Information about Subscribers' 2018 [229].

[917] 'Pravila khraneniya informatsii ob abonentakh operatorami svyazi prinyaty v RK [The rules for storing information about subscribers by telecom operators are taken in the Republic of Kazakhstan]' (*Zakon.kz*, 3 May 2018) <https://www.zakon.kz/4916698-pravila-hraneniya-informatsii-ob.html> accessed 28 June 2019.

[918] David Kaye Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (n 792) para 58.

explained in part by virtue of the remaining ties in the area after dissolution of the Soviet Union. Prior to the collapse, the KGB (USSR Committee for State Security) had extensive financing at its disposal for research; however, as its successor, the FSB was provided with only a tenth of that budget. This resulted in a number of developers and researchers preferring to act in the private sector.[919] Therefore, being composed of former KGB employees, many of the newly emerging tech firms had long-time connections to the FSB, which provided a basis for the current collaboration. Additionally, before the breakup of the union, the KGB had an extensive chain of regional branches in the Soviet states. Many of these bodies were transformed into security agencies in independent republics, and continued to adhere to the FSB approach, taking similar legislative initiatives and sharing technologies and the concepts of 'information security'.[920]

According to Kerr, at least nine of the FSU republics mimic Russian technological, legal, and institutional frameworks relating to online surveillance.[921] While some legal and technical developments have been adopted over the last several decades, many updates occurred around the 2010s, probably as a response to the growing role of online media in revolution-type events. In the 2000s, for instance, Ukraine, Moldova, and Ukraine − emulating the Russian approach − formed specialised counter-computer crime units (Department 'K') under the auspices of their Interior Ministries.[922]

As for shared interception technologies, the author refers primarily to the System for Operative Investigative Measures (SORM), which is the technical equipment used to carry out operational investigative activities involving telephone, mobile, and wireless

[919] Peter Bourgelais, 'Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia' [2013] Access Now <https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf> accessed 5 September 2019.

[920] Soldatov and Borogan (n 375).

[921] The only exceptions are Georgia, Armenia, and the Baltic States; Kerr (n 364).

[922] Rafal Rohozinski and Vesselina Haralampieva, 'Internet Filtering in the Commonwealth of Independent States 2006-2007' (*OpenNet Initiative*, 2007) <https://opennet.net/studies/cis2007> accessed 6 September 2019.

communication networks. To establish a monitoring infrastructure, Internet service providers are obliged to install 'Control Points' on their networks – which serve as a 'black boxes' on communication facilities – and to connect each node to FSB centres.[923]

The system was developed in Russia in the late 1990s, and was replicated shortly thereafter in other post-Soviet countries. Initially, SORM covered telephone data and was accessible only by the Federal Security Service (FSB). However, in subsequent years the system provided for Internet traffic as well, and the list of equipped law enforcement bodies became longer.

The most current release of the SORM-3 system collects data from all devices, and ensures their long-term storage. In this manner, authorities have are enabled to undertake targeted surveillance of all personal communication, including landline and mobile phones as well as Internet traffic.

In Russia, the FSB and the police have had access to Internet traffic since 2000. The Ministry of Communication ordered ISPs to install SORM-2,[924] and law enforcement bodies were not required to provide any information to operators, such as targets or involving permission to conduct surveillance.

Uzbekistan's national security service implemented SORM in 2006, purportedly to combat extremism and terrorism.[925] Internet and mobile providers were required to install equipment in order to be licensed. The law prohibited providers from revealing the specifics of surveillance methods.

---

[923] Kerr (n 364).

[924] Order of the Ministry of Communications of the Russian Federation 'On the Procedure for Implementing a System of Technical Means for Ensuring Operational-Search Measures on Telephone, Mobile and Wireless Communication Networks and Personal Radio Calls' 2000 [130].

[925] Resolution of the President of the Republic of Uzbekistan 'On measures to improve the efficiency of the organization of operational search activities on telecommunications networks of the Republic of Uzbekistan' 2006 [PP-513].

Belarusian authorities applied SORM technology in 2010, which granted access to communication data.[926] Moreover, the authorities used the Russian-developed software Semantic Archive for monitoring open web data, such as sites, blogs, forums, online databases, and file archives. On several occasions, the government employed viruses, malware, and spy software for the purpose of cyber surveillance.[927]

Kyrgyzstan authorities have employed every version of SORM, with updates to SORM-2 and SORM-3 being conducted in 2012 and 2014, respectively.[928] According to the latest regulations, ISPs and mobile operators are required to store user data for a maximum of three years. In turn, the authorities are provided with direct, real-time access to personal communication.

In July 2014, the Russian Ministry of Communication ordered ISPs to upgrade to the latest version of SORM.[929] Some sources suggest that the new equipment has a Deep Package Inspection (DPI) capability.[930]

Kazakhstan's surveillance network was also constructed on the basis of Russia's SORM technology.[931] The National Security Committee has recently developed new technical regulations for SORM, which came into effect in January 2018. Whereas the need to implement the document was attributed to matters involving national security and anti-

[926] Stanislav Budnitsky, 'Digital Eurasia: Big brother in Eurasia' (*Digital Report*, 13 November 2014) <https://digital.report/digital-eurasia-big-brother-eurasia/> accessed 5 July 2019; Soldatov and Borodan (n 397).
[927] 'Insights into Internet Freedom in Central Asia: Belarus' (*Digital Defenders Partnership*) <https://www.digitaldefenders.org/belarus/> accessed 5 July 2019.
[928] 'Instruction on the Procedure for Interaction of Telecommunication Operators and Mobile Cellular Operators with State Bodies of the Kyrgyz Republic Engaged in Operational Investigative Activities (Approved by the Decree of the Government of the Kyrgyz Republic No. 360)' (*Ministry of Justice*, 30 June 2014) <http://cdb.minjust.gov.kg/act/view/ru-ru/96622?cl=ru-ru> accessed 5 July 2019.
[929] 'SORM-3 Budet Vnedren Do 31 Marta 2015 Goda [SORM-3 Shall Be Implemented by March 31, 2015]' (*Roskomsvoboda*, 11 October 2014) <https://roskomsvoboda.org/8827/> accessed 5 July 2019.
[930] Nathalie Maréchal, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' (2017) 5 Media and Communication 29.
[931] Order of the Chairman of the National Security Committee of the Republic of Kazakhstan 'On approval of the technical regulation 'General requirements for telecommunications equipment to ensure the conduct of operational-search activities, collection and storage of service information about subscribers' 2016 [91].

terrorism, the experts were concerned about potential misuse with respect to privacy and freedom of expression.[932] At the same time, the media noted that such practices are common in international practice, as exemplified by the US PATRIOT Act of 2001 and similar initiatives throughout the European states.[933]

Yet another example of the use of Russian surveillance equipment in the regions in question may be attributed to Ukraine, as several sources have suggested that the Ukrainian government used SORM equipment.[934] However, the extent to which technology was implemented remains unclear. In December 2013, the national regulator of communication (NCCIR) introduced new rules for the area. The problematic provision required ISPs to install all technical means for investigative activities.[935]

Since surveillance practices constitute interference with the right to freedom of expression and associated human rights, governments must ensure an appropriate balance. The relevant approaches and recommendation were covered under Section 6.3, *'Procedures and Measures as Enshrined in Legislation and Practice: Towards Total Deanonymisation'*. The general recommendations as to applying states' surveillance practices is to follow the principles of legality, legitimacy, and proportionality; to take narrow measures and on a case-specific basis; and to ensure the transparency of the process and the possibility of an independent judiciary authority challenging the decision.

---

[932] 'Telefonnyye razgovory kazakhstantsev budut zapisyvat' i khranit' [Kazakhstani telephone conversations will be recorded and stored]' (*NUR.KZ*, 19 May 2017) <https://www.nur.kz/1498984-telefonnye-razgovory-kazakhstancev-b.html?> accessed 20 September 2019; Daria Maksimova, 'Zakonna li proslushka abonentov sotovykh operatorov RK? [Is wiretapping of subscribers of RK by mobile operators legal?]' (*Kursiv*) <https://kursiv.kz/news/vlast-i-biznes/2017-05/zakonna-li-proslushka-abonentov-sotovykh-operatorov-rk> accessed 20 September 2019.

[933] 'Telefonnyye razgovory kazakhstantsev budut zapisyvat' i khranit' [Kazakhstani telephone conversations will be recorded and stored]' (n 932); Maksimova (n 932).

[934] Soldatov and Borogan (n 375); Kerr (n 364).

[935] Oleg Shynkarenko, 'Zashmorh Na Internet [A Noose on the Internet]' (8 January 2014) <http://www.theinsider.ua/business/52bac42dd8f4d/> accessed 7 July 2019.

6.4.2. Remote Control System and Other Surveillance Equipment

In February 2014, Citizen Lab suspected 20 governments of using the advanced computer spyware Remote Control System (RCS).[936] RCS was developed by the Milan-based firm Hacking Team, and fell into disrepute because it had helped governments to spy on their opponents The spyware enabled remote access to webcams and microphones, stealing any data from computers and monitors, and interfering with Internet traffic as well as breaking into encrypted messages.

The state agencies from Azerbaijan, Kazakhstan, Uzbekistan,[937] and Russia[938] were alleged to be Hacking Team clients, and these suspicions were confirmed in 2015 following a Hacking Team data breach.[939]

Earlier in 2013, Reporters Without Borders called Hacking Team one of the 'corporate enemies of the Internet' for cooperating with repressive governments. The company, however, denied any purchases of RCS by authoritarian regimes.

Examples of digital surveillance technologies are not limited to SORM or to RCS. Since January 2016, for instance, the Kazakh government has required all netizens to install a 'national security certificate'.[940] The certificate grants authorities the power to overcome secure connections and encrypted traffic, and to have access to a user's browsing history.

---

[936] Bill Marczak and others, 'Mapping Hacking Team's "Untraceable" Spyware' (*The Citizen Lab*, 17 February 2014) <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/> accessed 7 July 2019.
[937] '"We Will Find You, Anywhere": The Global Shadow of Uzbekistani Surveillance' (Amnesty International 2017) EUR 62/5974/2017 <https://www.amnesty.org/download/Documents/EUR6259742017ENGLISH.PDF>.
[938] Alex Hern, 'Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim' *The Guardian* (6 July 2015) <https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim> accessed 7 July 2019.
[939] ibid.
[940] Regulations made under the Law on Communications.

According to the initial announcement, citizens are required to install the certificate on all devices.[941]

In July 2016, the Belarusian Investigative Committee publicly confirmed its use of a Japanese monitoring system. Called Cellebrite's UFED Touch, the system provides access to smartphone data, even − in some cases − when it involves a locked, switched off, or broken device.[942]

Following protests in Belarus in the spring of 2017, President Lukashenko approved creation of the Security Monitoring System.[943] The system undertakes video monitoring and collects data in real time.[944]

In Section 6.3*, 'Procedures and Measures as Enshrined in Legislation and Practice: Towards Total Deanonymisation'*, the author covered recommendations developed by international organisations with regard to surveillance practices. Generally, the states are recommended to strictly limit surveillance, and to resort to such measures only in exceptional circumstances. The decisions are required to be implemented on the principles of legality, legitimacy, and proportionality, and supervised by independent judiciary bodies.

---

[941] Adil Nurmakov, 'Eksperty: Kazakhstan nameren sledit' za zashchishchennym trafikom pol'zovateley [Experts: Kazakhstan intends to monitor the protected traffic of users]' (*Digital Report*, 4 December 2015) <https://digital.report/kz-security-certificate-surveillance/> accessed 7 July 2019.

[942] Andrei Gavron, 'Minskiye sledovateli obzavelis' kompleksom po izvlecheniyu dannykh iz smartfonov [Minsk investigators acquired a complex to extract data from smartphones]' (*Minsk News*, 22 July 2016) <https://minsknews.by/minskie-sledovateli-obzavelis-kompleksom-po-izvlecheniyu-dannyih-iz-smartfonov/> accessed 7 July 2019.

[943] Decree No. 187 "On the Republican Public Security Monitoring System"

[944] 'Commentary to Decree No. 187 of 25 May 2017' (*Official Internet Portal of the President of the Republic of Belarus*, 26 May 2017) <http://president.gov.by/en/news_en/view/commentary-to-decree-no-187-of-25-may-2017-16293/> accessed 7 July 2019; 'Belarus Rolls Out Big Brother to Counter Worst Unrest in Decades' (27 March 2017) <https://www.bloomberg.com/news/articles/2017-03-27/belarus-rolls-out-big-brother-to-counter-worst-unrest-in-decades> accessed 7 July 2019.

6.5. Procedures and Measures as Enshrined in Legislation and Practice: Compartmentalising the Web

6.5.1. Obligatory Use of Local Domain Names

As early as 2005, the Kazakh government required all websites in the .kz domain to use Kazakhstan's hosting services.[945] In late 2010, authorities took steps to apply this regulation to Google,[946] causing the engine to redirect traffic from Google.kz to Google.com. The company stressed that localisation requirements would help to create a 'fractured Internet'.[947] Soon afterwards, the government explained the regulations,[948] stating that the rule was to be applied only to domains registered after September 7, 2010. In this manner, Google.kz was re-launched.[949]

Since 2010, Belarusian authorities have required all domestically registered – .by – domain names to operate on local hosting services.[950] The provision was introduced in line with Presidential Decree No. 60,[951] which strengthened the regulation of BYnet.

Law No. 317-3 regulated the activities of commercial organisations in the .by domain and in the national segment of the Internet, and entered into force on January 6, 2012.[952] In particular, paragraph 22.16 imposes fines on Belarusian organisations that sell goods or provide services via websites located outside the country. It should be noted that the

---

[945] Chander and Lê (n 518).
[946] Government required Google to comply with Order of the Minister of Communications and Information of the Republic of Kazakhstan 2010 [220].
[947] 'Changes to the Open Internet in Kazakhstan' (*Official Google Blog*, 7 June 2011) <https://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html> accessed 4 July 2019.
[948] 'Announcement of the Kazkahstani Association of IT Companies' (8 June 2011) <https://nic.kz/docs/announc_14_06_2011.jsp> accessed 4 July 2019.
[949] 'Google.Kz Vernulsya v Kazakhstan [Google.Kz Returned to Kazakhstan Google.Kz]' (*Tengrinews*, 15 June 2011) <https://tengrinews.kz/internet/Googlekz-vernulsya-v-kazahstan-190571/> accessed 4 July 2019.
[950] Decree of the Council of Ministers 'On Some Questions of Improving Usage of the National Segment of the Global Internet Computer Network' 2010 [644].
[951] Decree of the President of the Republic of Belarus 'On measures to improve the use of the national segment of the Internet' (n 686).
[952] The Law 'On Amendments to the Code of the Republic of Belarus on Administrative Offenses and the Procedural-Executive Code of the Republic of Belarus on Administrative Offenses' 2011 [317-3].

requirement does not apply to retailers located abroad and selling goods/services to Belarusian customers.

6.5.2. Data Localisation

In Russia, the data localisation law entered into force in September 2015.[953] The law obliged foreign companies to keep the personal data of Russian citizens on local servers. Shortly afterwards, the state Internet watchdog, Roskomnadzor, began to audit compliance with the new legislation.[954] Many domestic and international companies transferred the information to Russian data centres; for example, eBay, PayPal, Viber,[955] AliExpress,[956] Apple,[957] and Google[958] all complied with the law.

At the same time, several popular social media and messaging platforms were blocked for violating data localisation requirements. This disturbing trend began in November 2016 with the banning of the global recruiting website LinkedIn.[959]

---

[953] Federal Law 'On Amending Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Procedure for Processing Personal Data in Information and Telecommunication Networks' 2014 [242-FZ]; Matthew Newton, and Julia Summers, 'Russian Data Localization Laws: Enriching "Security" & the Economy' (*The Henry M. Jackson School of International Studies*, 28 February 2018) <https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/> accessed 4 July 2019.

[954] Lisa Baird, 'Russia to Increase Data Audits in 2016 With Data Localization Law & More News on The EU's Safe Harbor Ruling' (*Life Sciences Legal Update*, 8 January 2016) <https://www.lifescienceslegalupdate.com/2016/01/articles/industry-developments/russia-to-increase-data-audits-in-2016-with-data-localization-law-more-news-on-the-eus-safe-harbor-ruling/> accessed 4 July 2019.

[955] 'Messaging App Viber Reportedly Bows to Russian Data-Localization Law, Relocates User Data to New Servers' (*Meduza*, 19 October 2015) <https://meduza.io/en/news/2015/10/19/messaging-app-viber-reportedly-bows-to-russian-data-localization-law-relocates-user-data-to-new-servers> accessed 4 July 2019.

[956] 'AliExpress to Open Representation in Russia and Comply with Personal Data Storage Law' (*East-West Digital News*, 21 March 2017) <https://www.ewdn.com/2017/03/21/aliexpress-to-open-representation-in-russia-and-comply-with-personal-data-storage-law/> accessed 4 July 2019.

[957] 'Apple Provides Details on Compliance with Russian Data-Localization Law' (*East-West Digital News*, 5 February 2019) <https://www.ewdn.com/2019/02/05/apple-provides-russian-authorities-with-details-on-compliance-with-data-localization-law/> accessed 4 July 2019.

[958] Olga Razumovskaya, 'Google Moves Some Servers to Russian Data Centers' *Wall Street Journal* (10 April 2015) <https://www.wsj.com/articles/google-moves-some-servers-to-russian-data-centers-1428680491> accessed 4 July 2019.

[959] Irina Chevtaeva, 'Blokirovka LinkedIn v Rossii Priznana Zakonnoy [LinkedIn Ban in Russia Is Recognized as Legal]' (*Vedomosti*, 10 October 2016) <https://www.vedomosti.ru/technology/articles/2016/11/10/664394-blokirovka-linkedin> accessed 4 July 2019.

In April 2017, Roskomnadzor blocked the walkie-talkie app Zello. But what was the background? Does it mention state security? Alexey Gavrilov, Zello's CTO and founder, called the regulations 'senseless'.[960] Notably, the app was popular among truck drivers who were striking against increasing the road tax.[961]

In 2019, the law affected the largest international social media: Facebook and Twitter. In April 2019, both companies received a small fine of €40 for failing to report on the localisation progress. Authorities granted the platforms 9 more months to fulfill the requirements.[962]

Kazakhstan authorities adopted data localisation *vis-à-vis* local websites in 2016. According to amendments to the Informatisation Law, domestic companies are required to store personal information relating to Kazakhstan's citizens within the country.[963] In late 2017, authorities made public a plan to negotiate with international social media platforms and messaging apps to encourage them to operate on local services.[964]

A Belarusian decree on user-identification[965] imposed provisions on the storing of personal data. The owners of Internet pages were placed under the obligation to keep

---

[960] 'V Rossii nachali blokirovat' Zello. Chto eto i kto ot etogo postradayet? [Russia began to block Zello. What is it and who will suffer? Q&A on the app used by the protesting truckers]' (*Meduza*) <https://meduza.io/feature/2017/04/14/v-rossii-nachali-blokirovat-zello-chto-eto-i-kto-ot-etogo-postradaet> accessed 27 June 2019.

[961] Isaac Webb, 'Russia Blocks Walkie-Talkie App Zello As Truckers Strike' (*Global Voices*, 10 April 2017) <https://globalvoices.org/2017/04/10/russia-blocks-walkie-talkie-app-zello-as-truckers-strike/> accessed 27 June 2019.

[962] 'Facebook i Twitter dali yeshche devyat' mesyatsev dlya lokalizatsii dannykh rossiyan v RF [Facebook and Twitter were given another nine months to localize Russian data in the Russian Federation]' (*Interfax.ru*, 16 April 2019) <https://www.interfax.ru/russia/658372> accessed 4 July 2019.

[963] Rhiannon Webster, 'Kazakhstan: Localization of Personal Data' (*DAC Beachcroft*, 1 January 2016) <https://www.dacbeachcroft.com/en/gb/articles/2016/january/kazakhstan-localization-of-personal-data> accessed 4 July 2019.

[964] 'Zarubezhnym sotssetyam vydvinut trebovaniya po razmeshcheniyu serverov v RK [Foreign social networks put forward requirements for the placement of servers in the Republic of Kazakhstan]' (*Profit.kz*, 2 November 2017) <https://profit.kz/news/42724/Zarubezhnim-socsetyam-vidvinut-trebovaniya-po-razmescheniu-serverov-v-RK/> accessed 4 July 2019.

[965] Decree of the Council of Ministers of the Republic of Belarus 'On the procedure for preliminary identification of users of the Internet resource, online media' (n 861).

identification data on Belarussian servers for the duration of the user agreement, as well as for a year from the date of its termination.

In June 2019, the Belarus Parliament approved a first reading of the draft law 'On personal data'.[966] In contrast to Russian legislation, the draft law does not demand that its citizens personal data be stored in the territory of the country. This means that there are no grounds for blocking foreign social networks and services in Belarus, which happened in Russia.

The critical overview of data nationalism practices as well as recommendations for national regulations were suggested by the Information Technology and Innovation Foundation.[967] The organisation compares economic isolationism with data isolationism: namely, the free flow of information is essential for trade and economic purposes, and it facilitates a greater transparency with respect to government surveillance practices. The Foundation notes that just like an economic nationalism, data nationalism would lead to poor economic outcomes. Additionally, the experts note that keeping data within local borders does not automatically guarantee its security, and therefore the necessity of the measure may be challenged. In line with this argument, ITIF offers two recommendations: 1) abandon any restrictions on the flow of data outside the borders; 2) adopt the 'Geneva Convention on the Status of Data', which provides for international standards regarding data access by authorities.[968]

[966] Pavliuk Bykovsky, 'Belarus' ne budet trebovat' khraneniya personal'nykh dannykh v strane [Belarus will not require the storage of personal data in the country]' (*DW.COM*, 13 June 2019) <https://bit.ly/2RRVW5v> accessed 4 July 2019.
[967] Castro (n 517) 10–11.
[968] In the ITIF's paper recommendation was addressed particularly for the US government, however, in the opinion of the author adopting international standards on data access is also relevant for analysed region.

6.5.3. Controlling Cross-Border Traffic

Since 2005, Uzbekistan has regulated use of the global net in academic institutions.[969] All scholarly and cultural organisations – e.g. schools, universities, libraries, and museums – are required to connect to the wider Internet exclusively through ZiyoNET, a national search engine that coordinates educational and youth-oriented sources.

Kazakh telecommunication operators may perform cross-border traffic exchanges only via a system named 'centralised management of telecommunication networks' (SCM). SCM − founded in 2008 and regulated by the State Technical Service − is a unified information system that allows real-time monitoring of a network. It contains, *inter alia*, information on the status of all key telecommunication facilities, backbone networks, and network traffic. Regulations regarding the centralised management of telecommunication networks were last amended in 2018.[970] Marat Asipov, editor-in-chief of Ratel.kz, called SCM the 'button that enables the easy banning of any open resource'.[971] This system is specifically a technical tool enabling authorities to conduct blockings.

In Belarus, permission for an exchange of international traffic is granted exclusively to the state-owned Beltelecom and the National Centre for Traffic Exchange.[972] Therefore, private operators are forced to buy access to an external Internet gateway through Beltelcom. The National Centre conducts the technical monitoring of any international traffic exchange

[969] Presidential Decree 'On the creation of a public educational information network of the Republic of Uzbekistan' 2005 [ПП-191-сон].
[970] Order of the Chairman of the National Security Committee of the Republic of Kazakhstan 'On approval of the Rules of operation of the system of centralized management of telecommunications networks of the Republic of Kazakhstan' 2018 [25].
[971] Marat Asipov, 'Kto Blokiruyet Neugodnyye Sayty v Kaznete [Who Blocks Unwanted Websites in Kaznet? Archieved]' (*Esquire*, 28 September 2015) <https://web.archive.org/web/20170402082300/https://www.esquire.kz/3128-kto_blokiruet_neugodnie_sayti_v_kaznete> accessed 4 July 2019.
[972] Order of the Operational Analytical Center under the President of the Republic of Belarus 'On approval of the list of telecommunication operators eligible for international traffic and accession to the telecommunication networks of foreign states' 2012 [91].

and connection to the telecommunication networks of foreign countries, and does this by providing access to traffic exchange points.

In May 2017, the President of Russia, Vladimir Putin, signed the 'Information Society Development Strategy', to be in force until 2030. The guidelines for this ICT policy contained provisions to increase Runet autonomy: for instance, 'to replace imported equipment, software and the electronic component base with Russian counterparts, and to ensure technological and production independence and information security'. [973] The document called for, *inter alia*, an assurance that Russian 'cultural and spiritual values' would be respected during the use of ICTs.[974]

In 2019, Russian lawmakers approved a law on autonomous operation of the Internet.[975] The law was a response to the US national cybersecurity strategy adopted in September 2018. Because in this strategy Russia was accused of cyber attacks, the authorities considered that the country could potentially become disconnected from foreign servers.[976]

Most of this law's provisions will come into force on 1 November 2019. The document will require ISPs to install technical facilities, which, in the event of the Russian segment of the global network becoming isolated, will allow Roskomnadzor[977] to conduct centralised network management. For the rest of the time, the equipment will be used to

[973] Decree of the President of the Russian Federation 'On the Strategy for the development of the information society in the Russian Federation for 2017-2030' 2017 [203] 12.
[974] 'Russia's Approves Information Society Development Strategy through 2030' (*Meduza*, 10 May 2017) <https://meduza.io/en/news/2017/05/10/russia-s-approves-new-information-society-development-strategy-through-2030> accessed 5 July 2019.
[975] Federal Law 'On Amending the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Protection of Information' 2019 [90-FZ].
[976] 'Bill On Autonomous Operation Of Russia's Internet Submitted To Duma' (*RadioFreeEurope/RadioLiberty*, 14 December 2018) <https://www.rferl.org/a/bill-on-autonomous-operation-of-russia-s-internet-submitted-to-duma/29656655.html> accessed 5 July 2019.
[977] State Internet regulator.

block forbidden resources. The overall cost of the project,[978] as well as its technical capacities[979] for realisation, remains unclear.

As the author has noted in the previous section, interference with the free flow of information online has negative aspects with respect to a state's economic capacities, and can affect the security of citizens. Therefore, the states under scrutiny should take these notions into account when taking restrictive measures.

[978] 'Vizhu novosti, chto na izolyatsiyu interneta potratyat iz byudzheta to li pochti dva, to li 20 milliardov rubley. Tak skol'ko? (Spoyler: neizvestno) [I see the news that almost two, or 20 billion rubles will be spent on isolating the Internet from the budget. So, how much? (Spoiler: unknown)]' (*Meduza*, 7 February 2019) <https://meduza.io/feature/2019/02/07/vizhu-novosti-chto-na-izolyatsiyu-interneta-potratyat-iz-byudzheta-to-li-pochti-dva-to-li-20-milliardov-rubley-tak-skolko-spoyler-neizvestno> accessed 5 July 2019.

[979] Henry Foy and Max Seddon, 'Russian Technology: Can the Kremlin Control the Internet?' (*Financial Times*, 5 June 2019) <https://www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2> accessed 5 July 2019.

7. Conclusions

The Internet is a global system of interconnected computer networks, where data is accessible by means of an array of wired and wireless networking technologies. Owing to its architecture, the Internet comes as an open system – not susceptible to authorisations at either the 'producer of content' end or the 'consumer of content' end. Its invention offered an unheard of possibility to gain access to a body of information of an unprecedented size. Recently, Web 2.0 heralded a shift towards mass participation in content creation and social networking for billions of Internet users, helping to overcome temporal and spatial barriers, increasing participation, and fostering novel means of exchanging knowledge and information. Online communication in a broad sense can be characterised by the fact that a wide variety of content is made immediately available to anyone who can afford the relatively minimal cost of access, thereby allowing multi-way communication of views and ideas on a level playing field that offers equal opportunities for communication. This places legislators in a predicament in terms of regulating such a complex and all-encompassing technology.

One may argue that regulation of the Internet occurs between the two extremes. At one end are proponents of the utopian aspiration to make the Internet free of state intervention. At the other end are those who favour complete regulation of the online domain, similar to, or even more strictly than, traditional media, calling for licensing and otherwise regulating content production and complete deanonymisation on the part of users.

The balance between controlling the Internet sphere and freedom of expression demonstrates certain peculiarities across the countries studied in the present research: Armenia, Azerbaijan, Belarus, Estonia, Georgia, Kazakhstan, Kyrgyzstan, Russia, Ukraine, Uzbekistan.

It should be noted that the hypothesis involving the commonality of legislative interventions was only partially corroborated. Taking into account the nature of the findings, it would be reasonable to divide the countries into two groups.

The first group demonstrates a constant deterioration of online freedoms. In Russia, Belarus, and Central Asian countries, the legitimisation of questionable practices of curtailing expression online − and the methods − is similarly employed, and involves common techniques such as the takedown of information, deanonymisation, mass surveillance, and data nationalism. The ruling elites have virtually not changed – or changed very little − since the collapse of the Soviet Union (see Section 3.2, 'Regional authoritarianism'). These countries are considered to have a high degree of censorship, which has deteriorated to become the backdrop for large-scale protest movements across the globe.[980] Having already subdued traditional media, authoritarian and semi-authoritarian regimes in these countries have targeted the Internet as the last medium of free expression. At this stage of its historical travels, it is unclear whether Ukraine can be added to this group of countries: this state, taking steps towards democratisation after the 2014 Euromaidan Revolution, at times seems to have inherited Russia's own toolkit for the purpose of combatting Russian propaganda.[981]

The second group of countries (the Baltic States, recently admitted EU member states as well as Georgia and Armenia) fare better. In recent years, Georgia and Armenia have been adapting their legal systems in accordance with international legal standards, particularly with respect to regulations involving online expression. Along with other Baltic Countries, Estonia is considered to have achieved a positive environment for free expression, and is used in this work as a benchmark for legal regulations involving the online sphere. Notwithstanding

[980] The author refers to the Arab Spring uprisings, which were accompanied by an extensive use of social networks by protesters, but also by revolutions in the region: for instance, the Ukrainian Euromaidan of 2014. See 'Procedures and Measures as Enshrined in Legislation and Practice: Takedown of Information'

[981] Since 2015, hundreds of Russian websites have been banned in Ukraine for reasons of national security, including popular social media platforms, search engines, and other services. See 'Internet blacklists'.

regional variations, the findings in Section 6, *'Post-Soviet Region: Case Studies in Online Regulation',* demonstrate the clear similarities in legislative practices in the first group of countries under scrutiny, which may be summarised in three points.

Point One. Reasons involving considerations of national security consistently serve as the most common pretext for limiting free speech. A large body of evidence relating to this was reported by Freedom House, which indicated similar patterns in the over-use of anti-extremism legislation in Russia, [982] Belarus, [983] Kazakhstan, [984] Kyrgyzstan, [985] and Uzbekistan.[986] Behind the shield of 'protecting' citizens, the governments are reinforcing legal environments and granting regulative authorities unlimited power to combat any unwanted expression. Therefore, any critical expression *vis-à-vis* a leading regime becomes 'extremist', 'a threat to national security', and is 'inciting hatred and terrorism'. The current legal system in a number of former Soviet countries suffers from vague definitions of key national security terms, such as extremism and terrorism. This leads to overly broad implications regarding the laws.

Point Two. Since the beginning of the 2010s, these states have introduced increasingly restrictive legislative environments *vis-à-vis* online content − again under the official line of protecting citizens. The expansion of poorly and ambiguously drafted formulas with regard to the online sphere has resulted in wide-ranging 'collateral damage', affecting an extensive amount of legitimate content. In Russia, Belarus, Kazakhstan, and Uzbekistan, for instance, legislative amendments to Internet regulations have enabled the government to block oppositional media, international news sources, and bloggers who are critical of the ruling elites.

---

[982] 'Freedom on the Net 2018: Russia' (n 540).
[983] 'Freedom on the Net 2018: Belarus' (n 541).
[984] 'Freedom on the Net 2018: Kazakhstan' (n 542).
[985] 'Freedom on the Net 2018: Kyrgyzstan' (n 543).
[986] 'Freedom on the Net 2018: Uzbekistan' (n 544).

Point Three. Legislators in the countries of the first group selectively copycat urgent initiatives from international legal practice with respect to Internet regulation. The list includes data protection, data localisation, some fake news, and disinformation-related initiatives, forcing responsibility on private companies to monitor the content. In practice, these regulations commonly fail to meet international legal requirements, and they copy the 'worst practices' from other jurisdictions.[987]

It may be inferred that legislative frameworks in this first group of states have been inspired by a mix of influences: that is, they follow the initiatives of 'Old Democracies' as well as approaches from Russia and examples from other neighbours. However, it would be erroneous to assume that Russia is the 'mastermind' behind all the repressive online legislation in the region. Instead, its role rests in maintaining a conservative regional values agenda, which is attractive to authoritarian regimes and provides new legislative ideas for neighbouring countries. Notwithstanding the fact that there might be some support for restrictive regulations through regional entities and mutual agreements, the regimes under scrutiny need no encouragement to establish greater state control. Countries such as Uzbekistan or Turkmenistan 'need no direction from Russia or indeed China to clamp down on dissent but remain open to new methods of how to do so'.[988]

As to the countries that fall into the second group, the research found a more relaxed legal regime and a closer follow-up of best practices.

To summarise the conclusions, the author has identified a number of initiatives that legislators currently implement or could implement to further align their respective legislature with the best practices of online regulation. Based on the premises of legality,

[987] Hug (n 205).
[988] ibid.

legitimacy, and proportionality as regards restrictions to freedom of expression, the initiatives include but are not limited to:

- Ensuring clear and unambiguous wordings of key definitions relating to national security;
- Removing specific provisions on defamation of authorities from the scope of criminal violations;
- Not holding intermediaries liable for third-party content;
- Ensuring transparency in maintaining online blacklists of websites to which access is restricted on the basis of national security concerns (explicitly or otherwise);
- Abolishing the practices of extrajudicial blocking of websites, and making appeal procedures against such decisions readily available;
- Ensuring the in-country operation of independent non-government human rights organisations, including the ability to receive grants, donations, and other funding, as well as abolishing the practice of labelling organisations as ‘foreign agents’;
- Limiting the scope of blocking mechanisms to single webpages rather than blocking whole platforms;
- Not impeding the usage of anonymising and encryption tools online;
- Applying online surveillance only on an exceptional case-by-case basis and as narrowly as possible;
- Abandoning the practices of data nationalism (that is, keeping data within geographical state borders) and cross-border traffic control.

The important safeguards to preserve freedom of expression as a fundamental human right should be guided exclusively by ensuring legality, legitimacy, and proportionality in any considerations regarding such restrictions.

The field of Internet regulation is highly dynamic. Therefore, further research is required to analyse the practice of applying recently enacted legislative changes in the post-Soviet region, and to examine the emerging differences between various groups of countries in this geographical area.

Technical Glossary

Anonymisers/anonymous proxy: proxy servers that protect users' digital identity and certain private information.[989] By using such tools, Internet users can prevent their location being traced and their Internet history searched. Users may use anonymisers to partially limit government surveillance or identity theft, and to gain access to banned online content. Anonymisers can operate as a website or as software.

Proxy-services: computer servers that play an intermediary role between the Internet user and the destination server.[990] In other words, the impression is given that a user's Internet activities come from another location. It should be noted that not all proxy servers ensure online anonymity; most commonly, they cover only an IP address and search activities.[991]

Virtual Private Networks (VPNs): a service that establishes a private network across a public network: that is, it extends encrypted and secure connection across a less secure – public − network.[992] VPN applications include the protection of privacy and anonymity online, and the circumvention of Internet censorship, and so on. Generally, VPNs are considered to be more advanced tools *vis-à-vis* online privacy in comparison to proxy-services.[993]

---

[989] 'What Is Anonymizer? - Definition from Techopedia' (*Techopedia.com*) <https://www.techopedia.com/definition/23133/anonymizer> accessed 18 August 2019.
[990] 'What Is a Proxy Service? - Definition from Techopedia' (*Techopedia.com*) <https://www.techopedia.com/definition/31705/proxy-service> accessed 19 August 2019.
[991] Jason Fitzpatrick, 'What's the Difference Between a VPN and a Proxy?' (*How-To Geek*, 18 June 2019) <https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/> accessed 19 August 2019.
[992] Margaret Rouse, 'What Is a VPN? - Definition from WhatIs.Com' (*SearchNetworking*, February 2019) <https://searchnetworking.techtarget.com/definition/virtual-private-network> accessed 19 August 2019.
[993] Fitzpatrick (n 991).

Tor: software facilitating anonymous online communication, including users' search activities, locations, messages, and many other forms of communication.[994] The software name is an acronym for 'The Onion Router', the project's original name. User data are anonymised through self-titled technology called 'onion routing', which ensures multi-layer encryption (similar to the layers of an onion). In other words, user data are encrypted and then sent to multiple Tor relay points. The software is commonly used to avoid surveillance and traffic analysis, and is considered to be the most effective tool for this purpose. The tool also enables access to blocked online content.

Circumvention tools: a type of software, websites, and other tools to overcome censorship online, including proxy services, VPNs, Tor, and so on.

Blocking/filtering: a complex of measures to prevent Internet users from accessing certain online content. It can be performed with varying levels of complexity: geographical (IP) blockings, URL-based blocking, and DPI blocking.

IP and Protocol-Based Blocking: blocking of IP addresses so that certain lists of addresses stop corresponding with end users and vice versa.[995] This is a major blocking technique, and is particularly easy to implement within certain regions.[996] May be circumvented using proxies, VPNs, or Tor.

Deep Packet Inspection: DPI is an advanced means of monitoring Internet traffic. It analyses the content and header of each data packet transferred within a network, making

---

[994] Aditya Tiwari, 'Everything About Tor: What Is Tor? How Tor Works ?' (*Fossbytes*, 22 May 2017) <https://fossbytes.com/everything-tor-tor-tor-works/> accessed 19 August 2019.
[995] 'What Is IP Address Blocking? - Definition from Techopedia' (*Techopedia.com*) <https://www.techopedia.com/definition/3991/ip-address-blocking> accessed 19 August 2019.
[996] 'Internet Society Perspectives on Internet Content Blocking: An Overview' (*Internet Society*, March 2017) <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/> accessed 19 August 2019.

real-time decisions according to assigned rules.[997] In other words, DPI technology can monitor overall Internet flow according to various categories, such as keywords, size of the packets, image matching, and types of applications.[998] The technology is also capable of rerouting traffic from certain IP addresses. DPI interference can be bypassed using encryption tools such as VPNs and Tor.[999]

URL-Based Blocking: a filter that analyses Internet traffic and compares the URLs requested by users with a local list. According to the result, the filter will enable or deny access to the address. Under certain conditions, the measure may be effective if the content is stored between multiple services and/or servers.[1000] Even if an IP changes, the URL remains unchangeable. However, with more complicated or frequently changed URLs, this measure is vague. For instance, a webpage can have a general URL such as *name.com* but also *name.video*, *name1.com*, and so forth. In such a case, all URLs corresponding with the forbidden web source must be added to the filter. Users may bypass filters using encryption tools.

Platform-Based Blocking: apart from local ISPs, the authorities can request major search engines, social networks, and mobile stores to filter availability of the content. However, a request must be sent separately to every search engine provider.[1001] Additionally, if the result is removed − for instance, from Google France − it would not necessarily be removed from Google Germany. Users can bypass this type of filtering by using alternative search engines.

---

[997] Margaret Rouse, 'What Is Deep Packet Inspection (DPI)? - Definition from WhatIs.Com' (*SearchNetworking*, September 2017) <https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI> accessed 19 August 2019.
[998] 'Internet Society Perspectives on Internet Content Blocking: An Overview' (n 996).
[999] 'What Is Deep Packet Inspection?' (*CactusVPN*) <https://www.cactusvpn.com/beginners-guide-to-online-privacy/what-is-deep-packet-inspection/> accessed 19 August 2019.
[1000] 'Internet Society Perspectives on Internet Content Blocking: An Overview' (n 996).
[1001] ibid.

DNS-Based Content Blocking: this type of blocking is conducted by examining DNS (domain name) queries. In this case, a specialised DNS resolver checks domain names against a ban list. When users make requests for blacklisted domain names, the special server delivers modified information, such as notification that the source has been banned. DNS blocking can be circumvented by VPNs.[1002]

Domain name: is a unique set of characters that refers to the name of the web source.[1003] For instance, *google.com* would be a domain name of the Google search engine. In turn, the web source may have many sub domains: for example, *translate.google.com* would refer to the Google Translate service.

Data Encryption: 'in computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks'.[1004]

Meta Data: 'is data that describes other data. Meta is a prefix that in most information technology usages means "an underlying definition or description". Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier. For example, *author*, *date created* and *date modified* and *file size* are examples of very basic document metadata. Having the ability to filter through that metadata makes it much easier for someone to locate a specific document'.[1005]

[1002] ibid.
[1003] Jeremy Laukkonen, 'What a Domain Name Is and How It Works' (*Lifewire*, 12 August 2019) <https://www.lifewire.com/what-is-a-domain-name-2483189> accessed 19 August 2019.
[1004] Margaret Rouse, 'What Is Encryption? - Definition from WhatIs.Com' (*SearchSecurity*, May 2019) <https://searchsecurity.techtarget.com/definition/encryption> accessed 19 August 2019.
[1005] Margaret Rouse, 'What Is Metadata? - Definition from WhatIs.Com' (*WhatIs.com*, 2014) <https://whatis.techtarget.com/definition/metadata> accessed 19 August 2019.

Internet Protocol address (IP address): 'is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network. The IP address is the core component on which the networking architecture is built; no network exists without it. An IP address is a logical address that is used to uniquely identify every node in the network. Because IP addresses are logical, they can change. They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks, just like mail is sent to friends and relatives'.[1006]

Uniform Resource Locator (URL): address of a resource on the Internet, which indicates the location of a resource as well as the protocol used to access it.[1007]

[1006] 'What Is an IP Address? - Definition from Techopedia' (*Techopedia.com*) <https://www.techopedia.com/definition/2435/internet-protocol-address-ip-address> accessed 19 August 2019.
[1007] 'What Is a URL? - Definition from Techopedia' (*Techopedia.com*) <https://www.techopedia.com/definition/1352/uniform-resource-locator-url> accessed 8 October 2019.

Bibliography

Primary sources

Cases

Ahmet Yildirim v Turkey [2012] ECtHR 3111/10

Barthold v Germany [1985] ECtHR 8734/79

Brandenburg v Ohio [1969] US Supreme Court 395 U.S. 444

Decision of Yessil district court of Astana [2012] Yessil district court of Astana 2-122/11

Decision on interpretation of some provisions of the Articles 137 and 4452 of the Criminal Procedure Code of the Republic of Azerbaijan [2015] Plenum of Constitutional Court of the Republic of Azerbaijan AZE-1999-1-003

Delfi AS v Estonia [2015] Grand Chamber ECtHR 64569/09

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] CJEU C-293/12 and C-594/12

Editorial Board of Pravoye Delo and Shtekel v Ukraine [2011] ECtHR 33014/05

Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González [2014] CJEU C-131/12

Handyside v United Kingdom [1976] ECtHR 5493/72

Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging [2011] Special Tribunal for Lebanon STL-11-01/1

International Court of Justice, Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons 1996

KU v FINLAND [2008] ECtHR 2872/02

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary [2016] ECtHR (Fouth Section) 22947/13

Mcintyre v Ohio Elections Commission [1995] US Supreme Court 514 US 334

National Socialist Party of America v Village of Skokie [1977] U S Supreme Court 432 US 43

On the Application of the Law of the Russian Federation 'On Mass Media' by the Courts [2010] The Supreme Court Plenary of the Russian Federation 16

On the case law on the protection of the dignity and honor of the individual, as well as the business reputation of the individual and the legal entity [2009] the Supreme Court Plenary of Ukraine 1

Perrin v UK [2005] ECtHR 5446/03

Roman Zakharov v Russia [2015] ECtHR 47143/06

Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others [2016] CJEU C-203/15 and C-698/15

The Sunday Times v The United Kingdom [1979] ECtHR 6538/74

Legislation

American Convention on Human Rights 1969 [1144 UNTS 123]

Civil Code of Kyrgyz Republic 1996 [15]

Constitution of the Republic of Kazakhstan 2019

Code of the Republic of Kazakhstan on Administrative Offenses 2014 [235–V]

Council of the European Union, Council Decision concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine 2014 [2014/145/CFSP]

——, Council Implementing Regulation implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine 2014 [810/2014]

Criminal Code of Georgia 1999

Criminal Code of Kyrgyz Republic 1997 [68]

Criminal Code of Russian Federation 1996 [63-FZ]

Criminal Code of the Kyrgyz Republic 2017 [19]

Criminal Code of the Republic of Armenia 2003 [ZR-528]

Criminal Code of the Republic of Belarus 1999 [275-З]

Criminal Code of the Republic of Kazakhstan 2014 [226–V]

Criminal Code of Ukraine 2001 [2341–III]

'Collective Security Treaty' 1992

Decree of the Council of Ministers of the Republic of Belarus 'On the procedure for preliminary identification of users of the Internet resource, online media' 2018 [850]

Decree of the Council of Ministers ‘On Some Questions of Improving Usage of the National Segment of the Global Internet Computer Network’ 2010 [644]

Decree of the Government of the Kyrgyz Republic ‘On the Regulations on mobile radio telephone service’ 2014 [97]

Decree of the Government of the Republic of Kazakhstan ‘On approval of the Rules for communication operators for collection and storage of user service information’ (as amended on 28 April, 2018) 2010 [246]

Decree of the President of the Republic of Belarus ‘On approval of the National Security Concept of the Republic of Belarus’ 2010 [575]

Decree of the President of the Republic of Belarus ‘On measures to improve the use of the national segment of the Internet’ 2010 [60]

Decree of the President of the Russian Federation ‘On the Strategy for the development of the information society in the Russian Federation for 2017-2030’ 2017 [203]

Directive (EU) of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA 2017 [2017/541]

Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC 2006 [2006/24/EC]

‘Draft Bill No. 603170-7 ’On Amending to the Federal Law “On National Payment System” and the Federal Law “On the Central Bank of the Russian Federation”’ (*Duma.gov.ru*)

<https://sozd.duma.gov.ru/bill/603170-7> accessed 2 August 2019

EU Commission, Illegal and harmful content on the internet 1996 [COM (96) 487 final]

European Convention on Human Rights 1950

Federal Law ’On Amending Articles 10.1 and 15.4 of the Federal Law ‘On Information, Information Technologies and Protection of Information’ 2017 [241-FZ]

Federal Law ’On Amending Articles 10.4 and 15.3 of the Federal Law on Information, Information Technologies and Protection of Information and Article 6 of the Law on Mass Media 2017 [327-FZ]

Federal Law ‘On Amending Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Procedure for Processing Personal Data in Information and Telecommunication Networks’ 2014 [242-FZ]

Federal Law ’On Amending the Federal Law ‘On Communications’ and the Federal Law ‘On Information, Information Technologies and Protection of Information’ 2019 [90-FZ]

Federal Law ‘On Amending the Federal Law “On Information, Information Security and Data Protection” and Certain Legislation of the Russian Federation Concerning the Exchange of Information Using Telecommunication Networks’ 2014 [97-FZ]

Federal Law ’On Amending the Federal Law On Information, Information Technologies and Information Protection 2019 [30-FZ]

Federal Law ’On Amending the Federal Law ‘On Information, Information Technologies and Protection of Information’ 2013 [398-FZ]

Federal Law ‘On Amending the Federal Law “On Information, Information Technologies and Protection of Information”” 2017 [276-FZ]

Federal Law ‘On Amendments to Article 44 of the Federal Law “On Communications” and the Code of Administrative Offenses of Russian Federation’ 2013 [304-FZ]

Federal Law ‘On Amendments to Certain Legislative Acts of the Russian Federation’ 2015 [129-FZ]

Federal Law ‘On Amendments to the Code of Administrative Offenses of the Russian Federation’ 2017 [396-FZ]

Federal Law ‘On Amendments to the Code of Administrative Offenses of the Russian Federation’—— 2018 [155-FZ]

Federal law ‘On Amendments to the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation’ 2012 [141-FZ]

Federal Law ‘On Amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety’ 2016 [375-FZ]

Federal Law ’On amendments to the Federal Law ‘On Communication’ 2017 [245-FZ]

Federal Law ‘On Amendments to the Federal Law “On Counter-Terrorism” and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety’ 2016 [374-FZ]

Federal Law ’On Amening Article 15.3 of the Federal Law ‘On Information, Information Technologies and Protection of Information’ 2019 [31-FZ]

Federal Law ‘On changing the term of office of the President of the Russian Federation and the State Duma’ 2008 [6-FKZ]

Federal Law ‘On Combating Extremist Activity’ 2002 [114-FZ]

GUAM, 'Charter of Organization for Democracy and Economic Development' (*GUAM*, 22 April 2006) <http://guam-organization.org/en/charter-of-organization-for-democracy-and-economic-development-guam/> accessed 16 August 2019

Government Bill (Anti-terrorism Act) 2001 [C-36 (37–1)]

Investigative Activities (Approved by the Decree of the Government of the Kyrgyz Republic No. 360)' (*Ministry of Justice*, 30 June 2014) <http://cdb.minjust.gov.kg/act/view/ru-ru/96622?cl=ru-ru> accessed 5 July 2019

Law of Georgia 'On Amendments to the Criminal Code of Georgia' 2015 [3699-II c]

Law of the Republic of Azerbaijan on operational investigative activities 1999 [728-IQ]

Law of the Republic of Kazakhstan 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan Concerning the Activities of the Internal Affairs Bodies' 2014 [200–V]

Law of the Republic of Kazakhstan 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Countering Extremism and Terrorism' (as amended on February 27, 2017) 2016 [28–VI]

Law of the Republic of Kazakhstan 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Counter-Terrorism Issues' 2013 [63–V]

Law of the Republic of Uzbekistan 'On introducing amendments to some legislative acts of the Republic of Uzbekistan' 2014 [ЗРУ-373-son]

Law 'On making changes and additions to some laws of the Republic of Belarus' 2018 [128-Z]

Matviyenko V and others, 'Document Kit to the Draft Law No. 161450-7' (26 April 2017)

<https://sozd.duma.gov.ru/bill/161450-7> accessed 30 July 2019

NATO, The North Atlantic Treaty 1949 [34 UNTS 243]

On Amendments and Additions to the Resolution of the Government of the Republic of Kazakhstan from March 30, 2010 No. 246 'On Approval of the Rules for Telecommunications Operators to Collect and Store Service Information about Subscribers' 2018 [229]

Order of the Acting Minister for Investment and Development of the Republic of Kazakhstan, appendix 3 'Rules for the provision of Internet access services' (as amended on 28 May, 2018) 2015 [171]

Order of the Chairman of the National Security Committee of the Republic of Kazakhstan 'On approval of the Rules of operation of the system of centralized management of telecommunications networks of the Republic of Kazakhstan' 2018 [25]

Order of the Chairman of the National Security Committee of the Republic of Kazakhstan 'On approval of the technical regulation 'General requirements for telecommunications equipment to ensure the conduct of operational-search activities, collection and storage of service information about subscribers' 2016 [91]

Order of the General Director of the Uzbek Agency of Communication and Informatization 'On the Approval of the Rules for the Provision of Mobile Communication Services' 2009 [1990-son]

Order of the Minister of Communications and Information of the Republic of Kazakhstan 2010 [220]

Order of the Ministry of Communications of the Russian Federation 'On the Procedure for

Implementing a System of Technical Means for Ensuring Operational-Search Measures on Telephone, Mobile and Wireless Communication Networks and Personal Radio Calls' 2000 [130]

Order of the Operational Analytical Center under the President of the Republic of Belarus 'On approval of the list of telecommunication operators eligible for international traffic and accession to the telecommunication networks of foreign states' 2012 [91]

Order of the Uzbek Agency of Communication and Informatization 'On the Approval of the Provision of Access to the Internet in Public Areas' 2004 [216]

Ordinance 'Concerning prompt measures to counteract illegal drug trade' 2014 [No. 6]

Penal Code of Estonia 2001 [RT I, 19.03.2019, 3]

Presidential Decree 'On the creation of a public educational information network of the Republic of Uzbekistan' 2005 [ПП-191-сон]

Resolution of Operational Analytical Center under the President of the Republic of Belarus 'On the system of countering violations of traffic transmission on telecommunication networks' 2016 [55]

Resolution of the Council of Ministers of the Republic of Belarus 'On amendments and addenda to the Resolution from 17 August, 2006 No. 1055' 2009 [677]

Resolution of the Council of Ministers of the Republic of Belarus 'On Approving the Rules for the Provision of Telecommunication Services' 2006 [1055]

Resolution of the Council of Ministers of the Republic of Belarus 'On expert commissions for evaluating information products for the presence (absence) of signs of extremism' 2014 [810]

Resolution of the Government of Russian Federation ‘On Rules for Internet Users Identification by Instant Messaging Services’ 2018 [1279]

Resolution of the Government of the Republic of Kyrgyzstan ‘On Information Security Concept of Kyrgyzstan for 2019-2023’ 2019 [209]

Resolution of the Government of the Russian Federation ‘On the Rules for Providing Mobile Communication Services’ 2005 [328]

Resolution of the Human Rights Council ‘On The promotion, protection and enjoyment of human rights on the Internet’ 2012 [A/HRC/20/8]

Resolution of the Ministry of Internal Affairs of the Republic of Belarus, Operational Analytical Center under the President of the Republic of Belarus and the Ministry of Communication and Informatization of the Republic of Belarus ‘On the procedure for the confirmation of telecommunications operators information about the subscriber’ 2016 [211/11/9]

Resolution of the President of the Republic of Uzbekistan ‘On measures to improve the efficiency of the organization of operational search activities on telecommunications networks of the Republic of Uzbekistan’ 2006 [PP-513]

Resolution of the Security Council of the Republic of Belarus ‘On the Concept of Informational Security of the Republic of Belarus’ 2019 [1]

Resolution of the State Committee for Communications, Informatization and Telecommunication Technologies of the Republic of Uzbekistan ‘On introducing changes and additions to the Regulation on the procedure for providing access to the Internet in public facilities’ 2014 [79–mx]

Rules for the provision of Internet access services 2011 [1718]

Ruling of Cabinet of Ministers of the Republic of Uzbekistan ‘On measures to streamline the system of accounting for mobile devices in the Republic of Uzbekistan’ 2018 [847-son]

Ruling ‘On approval of the Regulations on the procedure for restricting access to information resources (their constituent parts) on the Internet’ 2015 [6/8]

Ruling ‘On the procedure for restricting (renewing) access to Internet resources’ 2018 [8/10/6]

‘Terms of Mobile Services (Annex)’ (24 February 2015) <//online.zakon.kz/Document/?doc_id=33812603> accessed 26 June 2019

Terrorism Act 2000 2000 [2000 c. 11]

The Constitution of the Russian Federation

The Decree of the President of the Russian Federation ‘On Informational Security Doctrine of the Russian Federation’ 2016 [646]

The Law of the Republic of Belarus ‘On introducing amendments and addenda to the Code of the Republic of Belarus on Administrative Offenses and the Procedure Executive Code of the Republic of Belarus on Administrative Offenses’ 2014 [120-Z]

The Law of the Republic of Belarus ‘On introducing amendments to the Criminal, Criminal Procedure, Criminal Executive Codes of the Republic of Belarus, the Code of the Republic of Belarus on Administrative Offenses and the Procedural Executive Code of the Republic of Belarus on Administrative Offenses’ 2015 [241-Z]

The Law of the Republic of Kazakhstan ‘On the National Security of the Republic of Kazakhstan’ 2012 [527–IV]

The Law of the Republic of Uzbekistan ‘On Principles and Guarantees on Access to Information’ 2002 [439–II]

The Law ‘On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of the Activities of Non-Profit Organizations Acting as a Foreign Agent’ 2012 [121-FZ]

The Law ‘On amendments to some legislative acts of the Republic of Kazakhstan on information and communication networks’ 2009 [178–IV]

The Law ‘On Amendments to the Code of the Republic of Belarus on Administrative Offenses and the Procedural-Executive Code of the Republic of Belarus on Administrative Offenses’ 2011 [317-3]

The Law ‘On Amendments to the Federal Law “On the Protection of Children from Information Harmful to their Health and Development” and certain legislative acts of the Russian Federation’ 2012 [139-FZ]

The Law ‘On Changes and Addenda to Some Legislative Acts of the Republic of Kazakhstan on Information and Communications’ 2017 [128–VI]

The Law ‘On guarantees of the activities of the President of the Kyrgyz Republic and the status of the ex-president of the Kyrgyz Republic 2003 [152]

The Law ‘On Telecommunications’ 2005 [45-Z]

The Law ‘On the Fundamental Guarantees for the Activities of the President of the Republic of Uzbekistan’ 2003 [480–II]

The Law ‘On the Status of the Deputy of the Legislative Chamber and Member of the Senate of the Oliy Majlis of the Republic of Uzbekistan’ 2004 [704–II]

‘Treaty on the Establishment of the Eurasian Economic Community’ (*Eurasian Economic Community*, 2000) <http://www.evrazes.com/docs/view/95> accessed 9 August 2019

‘Treaty on the Eurasian Economic Union’ (*Eurasian Economic Union*, 29 May 2014) <https://docs.eaeunion.org/en-us/Pages/DisplayDocument.aspx?s=bef9c798-3978-42f3-9ef2-d0fb3d53b75f&w=632c7868-4ee2-4b21-bc64-1995328e6ef3&l=540294ae-c3c9-4511-9bf8-aaf5d6e0d169&EntityID=3610> accessed 9 August 2019

‘Treaty on the Union of Belarus and Russia’ (*Official website of the Union State*, 1997) <http://www.soyuz.by/about/docs/dogovor3/> accessed 9 August 2019

UN General Assembly, Universal Declaration of Human Rights 1948 [217 A (III)]

——, International Covenant on Civil and Political Rights 1966 [999 UNTS 171]

United Nations, Charter of the United Nations 1945 [1 UNTS XVI]

United Nations Convention on the Law of the Sea (UNCLOS) 1982 [1833 UNTS 3; 21 ILM 1261]

Vienna Convention on Diplomatic Relations 1961 [500 UNTS 95]

Zheleznyak S, Krupennikov V and Mitrofanov A, ‘Document Kit to the Draft Law No. 263448-6’ (19 April 2013) <https://sozd.duma.gov.ru/bill/263448-6> accessed 30 July 2019

Secondary sources

Articles

Akdeniz Y, ‘To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression’ (2010) 26 Computer Law & Security Review 260

Al Maruf H and others, 'Human Behaviour in Different Social Medias: A Case Study of Twitter and Disqus', *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (IEEE 2015)

Allison R, 'Russia Resurgent? Moscow's Campaign to "Coerce Georgia to Peace"' (2008) 84 International affairs 1145

Antonov O and Galushko A, 'The common space of neo-authoritarianism in post-Soviet Eurasia' (*Baltic Worlds*, 5 March 2019) <http://balticworlds.com/the-common-space-of-neo-authoritarianism-in-post-soviet-eurasia/> accessed 16 July 2019

Arva BJ and Piazza JA, 'Spatial Distribution of Minority Communities and Terrorism: Domestic Concentration versus Transnational Dispersion' [2016] Defence and Peace Economics

Babie PT, 'Ukraine's Transition from Soviet to Post-Soviet Law: Property as a Lesson in Failed Regulation' [2016] U. of Adelaide Law Research Paper

Bader M, 'The Legacy of Empire: A Genealogy of Post-Soviet Election Laws' (2012) 37 Review of Central and East European Law 449

——, 'Democracy Promotion and Authoritarian Diffusion: The Foreign Origins of Post-Soviet Election Laws' (2014) 66 Europe-Asia Studies 1350

Balkin JM, 'The Future of Free Expression in a Digital Age' (2008) 36 Pepp. L. Rev. 427

Barak A, 'Proportionality and Principled Balancing' (2010) 4 Law & Ethics of Human Rights 1

Betts W, 'Third Party Mediation: An Obstacle to Peace in Nagorno Karabakh' (1999) 19 Sais Review 161

Bleich E, ‘Freedom of Expression versus Racist Hate Speech: Explaining Differences between High Court Regulations in the USA and Europe’ (2013) 40 Journal of Ethnic and Migration Studies 283

Bourgelais P, ‘Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia’ [2013] Access Now <https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf> accessed 5 September 2019

Bowring B, ‘Russia and Human Rights: Incompatible Opposites’ (2009) 1 Goettingen J. Int’l L. 257

Brown C, ‘The Cross-Fertilization of Principles Relating to Procedure and Remedies in the Jurisprudence of International Courts and Tribunals’ (2008) 30 Loy. LA Int’l & Comp. L. Rev. 219

Cali B, Koch A and Bruch N, ‘The Legitimacy of Human Rights Courts: A Grounded Interpretivist Analysis of the European Court of Human Rights’ (2013) 35 Hum. Rts. Q. 955

Cameron DR and Orenstein MA, ‘Post-Soviet Authoritarianism: The Influence of Russia in Its “Near Abroad”’ (2012) 28 Post-Soviet Affairs 1

Castro D, ‘The False Promise of Data Nationalism’ [2013] Information Technology and Innovation Foundation

Chander A and Lê UP, ‘Data Nationalism’ (2014) 64 Emory LJ 677

Chandra S and Bhonsle R, ‘National Security: Concept, Measurement and Management’ (2015) 39 Strategic Analysis 337

Cohen-Almagor R, ‘Internet History’ (2011) 2 International Journal of Technoethics 45

Cory N, ‘The Worst Innovation Mercantilist Policies of 2016’ [2017] ITIF <http://www2.itif.org/2017-worst-innovation-mercantilist-policies.pdf>

Cottle S, ‘Media and the Arab Uprisings of 2011’ (2011) 12 Journalism 647

Crenshaw M, ‘The Causes of Terrorism’ (1981) 13 Comparative politics 379

Diamond L, ‘Liberation Technology’ (2010) 21 Journal of Democracy 69

Duah E, ‘Internet Service Providers’ Monitoring Obligations: Recent Developments’ (2012) 6 Masaryk UJL & Tech. 207

Ekiert G, Kubik J and Vachudova MA, ‘Democracy in the Post-Communist World: An Unending Quest?’ (2007) 21 East European Politics and Societies 7

Fabbrini F, ‘Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States’ (2015) 28 Harv. Hum. Rts. J. 65

Fjäder C, ‘The Nation-State, National Security and Resilience in the Age of Globalisation’ (2014) 2 Resilience 114

Ford P, ‘Freedom of Expression through Technological Networks: Accessing the Internet as a Fundamental Human Right’ (2014) 32 Wis. Int’l LJ 142

Frändberg Å, ‘An Essay on the Systematics of Legal Concepts’ (1987) 31 Scandinavian Studies in Law 81

Galushko A, ‘Politically Motivated Justice in the Former Soviet Union: The Novel Concept of Two-Fold Constitutionalism in Post-Soviet States’ (2016) 7 QMLJ 149

Gans-Morse J, ‘Searching for Transitologists: Contemporary Theories of Post-Communist

Transitions and the Myth of a Dominant Paradigm' (2004) 20 Post-Soviet Affairs 320

Georgescua S, 'Geopolitical Changes in Caucasus After 1991' (2013) 3 Karabük Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 123

Goldsmith JL, 'Against Cyberanarchy' (1998) 65 The University of Chicago Law Review 1199

Gorenburg D, 'Regional Separatism in Russia: Ethnic Mobilisation or Power Grab?' (1999) 51 Europe-Asia Studies 245

Griffen S, 'Defamation and Insult Laws in the OSCE Region: A Comparative Study' [2017] Vienna: Organization for Security and Co-operation in Europe

Grossman EJ, 'Russia's Frozen Conflicts and the Donbas' (2018) 48 Parameters 51

Hale HE, 'The Parade of Sovereignties: Testing Theories of Secession in the Soviet Setting' (2000) 30 British Journal of Political Science 31

Helfer LR, 'The Successes and Challenges for the European Court, Seen from the Outside' (2014) 108 AJIL Unbound 74

Howie E, 'Protecting the Human Right to Freedom of Expression in International Law' (2018) 20 International journal of speech-language pathology 12

Kahn J, 'The Parade of Sovereignties: Establishing the Vocabulary of the New Russian Federalism' (2000) 16 Post-Soviet Affairs 58

Kahn J, 'What Is the New Russian Federalism?' [2001] Contemporary Russian Politics: A Reader 374

Kerr JA, 'Information, Security, and Authoritarian Stability: Internet Policy Diffusion and

Coordination in the Former Soviet Region' (2018) 12 International Journal of Communication 3814

Kikstra J, 'Authoritarian Regimes and Innovation: A Case Study' [2016] University College Twente <https://www.researchgate.net/publication/318404915_Authoritarian_regimes_and_innovation_a_case_study> accessed 5 October 2019

Kilburn D and Earley J, 'Disqus Website-Based Commenting as an e-Research Method: Engaging Doctoral and Early-Career Academic Learners in Educational Research' (2015) 38 International Journal of Research & Method in Education 288

Komen MM, 'Homegrown Muslim Extremism in the Netherlands: An Exploratory Note' (2014) 7 Journal of Strategic Security 47

Kowalik-Bańczyk K and Pollicino O, 'Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information' (2016) 17 German Law Journal 315

Krieger T and Meierrieks D, 'What Causes Terrorism?' (2011) 147 Public Choice 3

Kudelia S, 'The Donbas Rift' (2017) 58 Russian Social Science Review 212

Kyj MJ, 'Internet Use in Ukraine's Orange Revolution' (2006) 49 Business Horizons 71

LaFree G and Dugan L, 'Introducing the Global Terrorism Database' (2007) 19 Terrorism and Political Violence 181

Laruelle M, 'Russia as a "Divided Nation," from Compatriots to Crimea: A Contribution to the Discussion on Nationalism and Foreign Policy' (2015) 62 Problems of Post-Communism 88

Lim M, 'Clicks, Cabs, and Coffee Houses: Social Media and Oppositional Movements in

Egypt, 2004–2011' (2012) 62 Journal of communication 231

Linderfalk U, 'Cross-Fertilisation in International Law' (2015) 84 Nordic Journal of International Law 428

MacFarlane SN, 'On the Front Lines in the near Abroad: The CIS and the OSCE in Georgia's Civil Wars' (1997) 18 Third World Quarterly 509

Maréchal N, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' (2017) 5 Media and Communication 29

Matveeva A, 'Radicalisation and Violent Extremism in Kyrgyzstan: On the Way to the Caliphate?' (2018) 163 The RUSI Journal 30

Matveeva A, Savin I and Faizullaev B, 'Kyrgyzstan: Tragedy in the South' (2012) 17 Ethnopolitics Papers

Mazloomi E, Yeoh EK-K and Karim MA, 'From Status Inconsistency to Revisionism: Russian Foreign Policy after Color Revolutions' (2018) 19 Japanese Journal of Political Science 489

McGonagle T, '"Fake News" False Fears or Real Concerns?' (2017) 35 Netherlands Quarterly of Human Rights 203

Meister S and Puglierin J, 'Perception and Exploitation: Russia's Non-Military Influence in Europe' (2015) 10 DGAP kompakt

Meraz S and Papacharissi Z, 'Networked Gatekeeping and Networked Framing On# Egypt' (2013) 18 The international journal of press/politics 138

Moga TL and Alexeev D, 'Post-Soviet States Between Russia and the EU: Reviving Geopolitical Competition? A Dual Perspective' (2013) 13 Connections 41

Moore C, ‘Foreign Bodies: Transnational Activism, the Insurgency in the North Caucasus and “Beyond”’ (2015) 27 Terrorism and Political Violence 395

Morozova N, ‘Geopolitics, Eurasianism and Russian Foreign Policy under Putin’ (2009) 14 Geopolitics 667

Moshes A and Rácz A, ‘What Has Remained of the USSR: Exploring the Erosion of the Post-Soviet Space’ (Finnish Institute of International Affairs 2019) 58 <https://www.fiia.fi/wp-content/uploads/2019/02/fiia_report58_what_has_remained_of_the_ussr_web.pdf> accessed 12 September 2019

Munir AB and others, ‘Data Retention Rules: A Dead End’ (2017) 3 Eur. Data Prot. L. Rev. 71

O’Loughlin J and Talbot PF, ‘Where in the World Is Russia? Geopolitical Perceptions and Preferences of Ordinary Russians’ (2005) 46 Eurasian Geography and Economics 23

Osakwe C, ‘Anatomy of the 1994 Civil Codes of Russia and Kazakstan: A Biopsy of the Economic Constitutions of Two Post-Soviet Republics’ (1997) 73 Notre Dame L. Rev. 1413

Papava V, ‘The Eurasianism of Russian Anti-Westernism and the Concept of “Central Caucaso-Asia”’ (2013) 1 Ideology and Politics 68

Pollicino O and Soldatov O, ‘Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context’ (2018) 19 German Law Journal 85

Puchooa P, ‘Defining Terrorism at the Special Tribunal for Lebanon’ [2011] Journal of Terrorism Research

Rapoport DC, ‘The Four Waves of Rebel Terror and September’ (2002) 8 Anthropoetics

Rengel A, ‘Privacy as an International Human Right and the Right to Obscurity in Cyberspace’ (2014) 2 Groningen Journal of International Law 33

Rød EG and Weidmann NB, ‘Empowering Activists or Autocrats? The Internet in Authoritarian Regimes’ (2015) 52 Journal of Peace Research 338

Roper SD, ‘Regionalism in Moldova: The Case of Transnistria and Gagauzia’ (2001) 11 Regional & Federal Studies 101

Sedler RA, ‘An Essay on Freedom of Speech: The United States versus the Rest of the World’ [2006] Mich. St. L. Rev. 377

Shafee F, ‘New Geopolitics of the South Caucasus’ (2010) 4 Caucasian Review of International Affairs 184

Sidak JG, ‘Some Economics of Flag Burning and Jimi Hendrix’ (2016) 1 Criterion J. on Innovation 563

Simic P, ‘Russia and the Conflicts in the Former Yugoslavia’ (2001) 1 Southeast European and Black Sea Studies 95

Skriba A, ‘Russian Strategy towards the Post-Soviet Space in Europe: Searching for Balance between Economy, Security, and Great Power Attractiveness’ (2016) 40 Strategic Analysis 604

Slaughter A-M, ‘Judicial Globalization’ (1999) 40 Va. J. Int’l L. 1103

Soldatov O, ‘Half-Hearted Inception, Miserable Existence, and the Untimely Death of the Bloggers’ Register in Russia’ (2019) 52 Israel Law Review 61

Solomon Jr PH, ‘Gorbachev’s Legal Revolution’ (1990) 17 Can. Bus. LJ 184

Striegher J-L, ‘Violent-Extremism: An Examination of a Definitional Dilemma’ [2015] The Proceedings of [the] 8th Australian Security and Intelligence Conference 75

Suslov M, ‘“Russian World” Concept: Post-Soviet Geopolitical Ideology and the Logic of “Spheres of Influence”’ (2018) 23 Geopolitics 330

Synodinou T-E, ‘Intermediaries’ Liability for Online Copyright Infringement in the EU: Evolutions and Confusions’ (2015) 31 Computer Law & Security Review 57

Tapia-Valdes JA, ‘A Typology of National Security Policies’ (1982) 9 Yale J. World Pub. Ord. 10

Toft MD and Zhukov YM, ‘Denial and Punishment in the North Caucasus: Evaluating the Effectiveness of Coercive Counter-Insurgency’ (2012) 49 Journal of Peace Research 785

Vedaschi A and Lubello V, ‘Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective’ (2015) 20 Tilburg Law Review 14

Walker C and Conway M, ‘Online Terrorism and Online Laws’ (2015) 8 Dynamics of Asymmetric Conflict 156

Walter C, ‘Defining Terrorism in National and International Law’ (2004) 1 Terrorism as a Challenge for national and international Law: Security versus Liberty 24

Wilner AS and Dubouloz C-J, ‘Homegrown Terrorism and Transformative Learning: An Interdisciplinary Approach to Understanding Radicalization’ (2010) 22 Global Change, Peace & Security 33

——, ‘Transformative Radicalization: Applying Learning Theory to Islamist Radicalization’ (2011) 34 Studies in Conflict & Terrorism 418

Yunusov K, 'The Development of Legal Systems of Central Asian States' [2014] 2 Studii Europene 23

Monographies

Akdeniz Y, *Media Freedom on the Internet: An OSCE Guidebook* (OSCE Representative on Freedom of the Media 2016)

Akiner S, *Kyrgyzstan 2010: Conflict and Context* (Central Asia-Caucasus Institute 2016)

Akrivopoulou C and Psygkas A, *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices* (IGI Global 2011)

Alexander Y, Brenner EH and Krause ST, *Turkey: Terrorism, Civil Rights, and the European Union* (Routledge 2008)

Anderson N, *The Internet Police: How Crime Went Online, and the Cops Followed* (WW Norton & Company 2013)

Bartlett J, Birdwell J and King M, 'The Edge of Violence: A Radical Approach to Extremism' [2010] Demos 5

Benedek W and Kettemann MC, *Freedom of Expression and the Internet* (Council of Europe 2013)

Browne A, *The Retreat of Reason: Political Correctness and the Corruption of Public Debate in Modern Britain* (The Institute for the Study of Civil Society 2006)

Bugaĭ N, *The Deportation of Peoples in the Soviet Union* (Nova Publishers 1996)

Buzan B, *People, States, and Fear: The National Security Problem in International Relations*

(Wheatsheaf Books Brighton 1983)

——, *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Harvester Wheatsheaf 1991)

Cameron I, *National Security and the European Convention on Human Rights* (Martinus Nijhoff Publishers 2000)

Carr N, *The Big Switch: Rewiring the World, from Edison to Google* (WW Norton & Company 2008)

Castells M, *Networks of Outrage and Hope: Social Movements in the Internet Age* (John Wiley & Sons 2015)

Combs CC, *Terrorism in the Twenty-First Century* (Routledge 2017)

Conley HA and others, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Rowman & Littlefield 2016)

Cornell S and Jonsson M, *Conflict, Crime, and the State in Postcommunist Eurasia* (University of Pennsylvania Press 2014)

Denber R, *Bloodshed in the Caucasus: Violations of Humanitarian Law and Human Rights in the Georgia-South Ossetia Conflict* (Human Rights Watch 1992)

Diuk N and Karatnycky A, *The Hidden Nations: The People Challenge the Soviet Union* (William Morrow & Co 1990)

Drobizheva LM, Gottemoeller R and Kelleher CM, *Ethnic Conflict in the Post-Soviet World: Case Studies and Analysis* (ME Sharpe 1998)

Eltchaninoff M, *Inside the Mind of Vladimir Putin* (Oxford University Press 2018)

English R, *Armed Struggle* (Pan 2005)

Fagan A and Kopecký P, *The Routledge Handbook of East European Politics* (Routledge 2017)

Fukuyama F, *The End of History and the Last Man* (Free Press 1992)

Greer SC, *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, vol 88 (Council of Europe 1997)

Hall H (ed), *Terrorism: Strategies for Intervention* (The Haworth Press 2003)

Halligan B and Shah D, *Inbound Marketing.: Get Found Using Google, Social Media, and Blogs* (John Wiley & Sons 2009)

Hamilton D and Mangott G, *The New Eastern Europe: Ukraine, Belarus, Moldova* (Center for Transatlantic Relations Washington, DC 2007)

Haraszti M and others, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Mit Press 2010)

Heller M and Fox MB, *Corporate Governance Lessons from Transition Economy Reforms* (Princeton University Press 2006)

Holland A, Bavitz C and Hermes J, *Intermediary Liability in the United States* (Global Network of Interdisciplinary Internet & Society Research Centers (NoC) 2015)

Hug A (ed), *Sharing Worst Practice: How Countries and Institutions in the Former Soviet Union Help Create Legal Tools of Repression* (Foreign Policy Centre 2016)

Hughes J and Sasse G, *Ethnicity and Territory in the Former Soviet Union: Regions in Conflict* (Routledge 2014)

Kavanagh D and Riches C (eds), 'Askar Akayev', *A Dictionary of Political Biography* (Oxford University Press 2009) <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095358830> accessed 25 June 2019

King C, *The Moldovans: Romania, Russia, and the Politics of Culture* (Hoover Press 2013)

Kosienkowski M and Schreiber W, *Moldova: Arena of International Influences* (Lexington Books 2012)

Krasner SD, *Problematic Sovereignty: Contested Rules and Political Possibilities* (Columbia University Press 2001)

Legvold R and Wallander CA, *Swords and Sustenance: The Economics of Security in Belarus and Ukraine* (MIT Press 2004)

Lindgren S, *Digital Media and Society* (Sage 2017)

Lynch D, *Russian Peacekeeping Strategies in the CIS: The Case of Moldova, Georgia and Tajikistan* (Springer 1999)

Mälksoo L, *Russian Approaches to International Law* (Oxford University Press, USA 2015)

Military Operations in Low Intensity Conflict. Field Manual 100-20/Air Force Pamphlet 3-20 (Headquarters, Department of the Army and the Air Force 1990)

Minahan J, *The Former Soviet Union's Diverse Peoples: A Reference Sourcebook* (Abc-clio 2004)

Neumann PR, *Countering Online Radicalization in America* (Bipartisan Policy Center 2012)

Pariser E, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin UK 2011)

Paulauskas K, *The Baltics: From Nation States to Member States* (European Union Institute for Security Studies 2006)

Polian P, *Against Their Will: The History and Geography of Forced Migrations in the USSR* (Central European University Press 2003)

Richter A, *Post-Soviet Perspective on Censorship and Freedom of the Media* (UNESCO Moscow Office Moscow 2007)

Rogov S, *A Eurasian Strategy for Russia* (Institute for US and Canadian Studies 1998)

Rumer EB, *Russian Foreign Policy beyond Putin* (Routledge 2017)

Sageman M, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (University of Pennsylvania Press 2008)

Sammut D and Dvetkovski N, *The Georgia-South Ossetia Conflict* (Verification Technology Information Centre 1996)

Samuel P, *Huntington, The Clash of Civilizations and the Remaking of World Order* (Simon and Schuster 1996)

Shipley TG and Bowker A, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace* (Newnes 2013)

Soldatov A and Borogan I, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries* (Hachette UK 2015)

Southers E, *Homegrown Violent Extremism* (Elsevier Inc 2013)

Suny R, *The Revenge of the Past: Nationalism, Revolution, and the Collapse of the Soviet Union* (Stanford University Press 1993)

Talbott S, *The Russia Hand: A Memoir of Presidential Diplomacy* (Random House 2007)

Tambini D, Leonardi D and Marsden C, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (Routledge 2007)

Tsygankov AP, *Routledge Handbook of Russian Foreign Policy* (Routledge 2018)

United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes.* (United Nations 2012) <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>

Wessel RA, *The European Union's Foreign and Security Policy: A Legal Institutional Perspective*, vol 33 (Martinus Nijhoff Publishers 1999)

Wilson A, *The Ukrainians: Unexpected Nation* (Yale University Press 2015)

Chapters in Edited Books

Aklaev A, 'Causes and Prevention of Ethnic Conflict: An Overview of Post-Soviet Russian-Language Literature' [2003] Leadership and Conflict Resolution: The International Leadership Series 249

Bailes AJ, Baranovsky V and Dunay P, 'Regional Security Cooperation in the Former Soviet Area' (2007) 2007 SIPRI Yearbook 174

Bremmer I, 'The Post-Soviet Nations after Independence' [2006] After Independence: Making and Protecting the Nation in Postcolonial and Postcommunist States 141

Cottey A, 'The Other Europe: Regional Security Governance in Europe's East' in Shaun Breslin and Stuart Croft (eds), *Comparative regional security governance* (Routledge 2012)

DeBardeleben J, ‘The Impact of EU Enlargement on the EU-Russian Relationship’ in Roger E Kanet (ed), *A Resurgent Russia and the West : The European Union, NATO and Beyond* (Republic of Letters 2009)

Demakova E and Godzimirski JM, ‘Russian External Energy Strategy: Opportunities and Constraints’, *Dynamics of energy governance in Europe and Russia* (Springer 2012)

Parrott B, ‘Perspectives on Postcommunist Democratization’ in Karen Dawisha and Bruce Parrott (eds), *Democratic changes and authoritarian reactions in Russia, Ukraine, Belarus and Moldova*, vol 3 (Cambridge University Press 1997)

Petro NN, ‘The Russian Orthodox Church’ in Andrei P Tsygankov (ed), *Routledge handbook of Russian foreign policy* (Routledge 2018)

Pollicino O and Bassini M, ‘Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis’ in A. Savin and J. Trzaskowski (eds), *Research Handbook on EU Internet Law* (2014)

Pollicino O and Bassini M, ‘Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis’ in A. Savin and J. Trzaskowski (eds), *Research Handbook on EU Internet Law* (2014)

——, ‘The Law of the Internet between Globalisation and Localisation’ [2014] Transnational Law: Rethinking European Law and Legal Thinking, Cambridge UP 346

Pollicino O and Soldatov O, ‘Judicial Balancing of Human Rights Online’ in M Susi (ed), *Routledge Handbook on Digital Society* (Routledge 2019)

Sokolov A, ‘Russian Peace-Keeping Forces in the Post-Soviet Area’ (1997)

Stone A, ‘The Comparative Constitutional Law of Freedom of Expression’ in Tom Ginsburg

and Rosalind Dixon (eds), *The Comparative Constitutional Law* (Edward Elgar 2011)

Van Elsuwege P, 'The Law and Politics of Post-Soviet Constitutionalism' [2019] What has remained of the USSR. Exploring the erosion of the Post-Soviet Space 21

Official Sources

Barker C, 'Australian Government Measures to Counter Violent Extremism: A Quick Guide' (*Parliament of Australia*) <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1415/Quick_Guides/Extremism> accessed 10 August 2019

'Country Reports on Terrorism 2016: Georgia' (United States Department of State 2017) <https://www.refworld.org/docid/5981e43ea.html> accessed 14 September 2019

'Country Reports on Terrorism 2016: Kazakhstan' (United States Department of State 2017) <https://www.state.gov/reports/country-reports-on-terrorism-2016/> accessed 14 September 2019

'Country Reports on Terrorism 2016: Kyrgyz Republic' (United States Department of State 2017) <https://www.refworld.org/docid/5981e43013.html> accessed 14 September 2019

European Parliament, 'At a Glance: Regional Organisations in the Post-Soviet Space' (2015) <http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/545718/EPRS_ATA(2015)545718_REV1_EN.pdf> accessed 12 September 2019

European Union Ministers Bonn Declaration 1997

Federal Bureau of Investigation Counterterrorism Division, '(U//FOUO) The Radicalization Process: From Conversion to Jihad' (Federal Bureau of Investigation Counterterrorism Division 2006) https://cryptome.org/fbi-jihad.pdf

‘Filtering, Blocking and Take-down of Illegal Content on the Internet’ (*Council of Europe*, 20 December 2015) <https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet> accessed 3 August 2019

‘Final Report of the High Level Expert Group on Fake News and Online Disinformation’ (*European Commission*, 12 March 2018) <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation> accessed 20 June 2019

Government of Denmark, ‘A Common And Safe Future: An Action Plan To Prevent Extremist Views And Radicalisation Among Young People’ (Government of Denmark 2009) <https://strongcitiesnetwork.org/en/wp-content/uploads/sites/5/2017/02/A-common-and-safe-future-Danish-Action-Plan-to-prevent-extremism.pdf>

Government of the United Kingdom, ‘Counter-Extremism Strategy’ (Government of the United Kingdom 2015) Cm 9148 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470088/51859_Cm9148_Accessible.pdf

Human Rights Committee, Concluding observations on the second periodic report of Kazakhstan 2016 [CCPR/C/KAZ/CO/2]

‘Internet: Case-Law of the European Court of Human Rights’ (Council of Europe 2015) <https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> accessed 14 June 2019

Kaye D, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 2016 [A/71/373]

Kaye D, Report of the Special Rapporteur on the promotion and protection of the right to

freedom of opinion and expression, David Kaye 2015 [A/HRC/29/32]

Kiai M, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai: Mission to Kazakhstan 2015 [A/HRC/29/25/Add.2]

La Rue F, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 2011 [A /66/290]

La Rue F, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 2011 [A/HRC/17/27]

'Limited Elections Observation Mission: Republic of Uzbekistan – Presidential Elections, 29 March 2015' (OSCE 2015) <https://www.osce.org/odihr/elections/uzbekistan/148186?download=true> accessed 26 June 2019

NATO, Bucharest Summit Declaration 2008

NATO Standartization Office, *AAP-06 NATO Glossary of Terms and Definitions* (2018th edn, NATO Standartization Office 2018)

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union 2011 [2011/C 181/01]

Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, Letter to the United Nations addressed to the Secretary-General: Developments in the field of information and telecommunications in the context of international security 2011 [UN A/66/359]

‘Preventing Violent Extremism and Radicalisation in Australia’ (Attorney-General’s Department 2015) <https://www.livingsafetogether.gov.au/information/Documents/preventing-violent-extremism-and-radicalisation-in-australia.PDF> accessed 10 August 2019

Royal Canadian Mounted Police, ‘Radicalization - a Guide for the Perplexed’ (Royal Canadian Mounted Police 2009) <http://publications.gc.ca/site/eng/9.696861/publication.html> accessed 12 August 2019

‘Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization’ (19 November 2010) <https://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf> accessed 8 July 2019

The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others, Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda 2017 [FOM.GAL/3/17]

UN General Assembly, Measures to eliminate international terrorism (Report of the Working Group) [C.6/55/L.2]

UN General Assembly, Plan of Action to Prevent Violent Extremism 2015 [A/70/674]

UN General Assembly, Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism 2016 [A/HRC/33/29]

UN General Assembly, Resolution adopted by the General Assembly: Territorial integrity of Ukraine 2014 [A/RES/68/262]

UN Human Rights Committee, General comment No. 34. Article 19: Freedoms of opinion and expression 2011 [CCPR/C/GC/34]

UN Security Council, Letter dated 17 May 1994 from the Permanent Representative of Georgia to the United Nations addressed to the President of the Security Council 1994 [S/1994/583]

——, Resolution 2178 (2014) Adopted by the Security Council at its 7272nd meeting 2014 [S/RES/2178]

U. S. Department of State, '2016 Country Reports on Human Rights Practices - Azerbaijan' (U S Department of State 2017) <https://www.refworld.org/docid/58ec8a753.html> accessed 19 June 2019

Venice Comission, Opinion on the Referendum of 17 October 2004 in Belarus 2004 [CDL-AD(2004)029]

Venice Commission, Opinion on the Federal Law on Combating Extremist Activity of the Russian Federation 2012 [CDL-AD(2012)016]

Web Sources

'72 criminal proceedings of "anti-Ukraine" propaganda cases registered in 2015-2017' (*Net Freedom*, 23 October 2017) <https://netfreedom.org.ua/72-criminal-proceedings-of-anti-ukraine-propaganda-cases-registered-in-2015-2017/> accessed 14 September 2019

'101: SIM Card Registration' (*Privacy International*) <http://privacyinternational.org/explainer/2654/101-sim-card-registration> accessed 26 July 2019

‘Absurdopedia / Wikia’ (*Roskomsvoboda*, 11 November 2012) <https://roskomsvoboda.org/3323/> accessed 21 July 2019

Adil Soz Foundation, ‘LiveJournal Portal, Several Blogs Suspended’ (*IFEX*, 2 September 2011) <https://ifex.org/livejournal-portal-several-blogs-suspended/> accessed 22 June 2019

Agence France Presse, ‘Belarus Blocks Online Sites and Closes Shops to Stem Currency Panic’ *The Guardian* (21 December 2014) <https://www.theguardian.com/world/2014/dec/21/belarus-blocks-online-websites-shops-currency-panic-rouble> accessed 14 September 2019

Ahmetov A, ‘Kazakhstantsev mogut arestovat’ za chuzhiye kommentarii na ikh stranitsakh v sotssetyakh [Kazakhstanis can be arrested for the comments of others on their pages in social networks]’ (*Tengrinews.kz*, 21 October 2015) <https://tengrinews.kz/kazakhstan_news/kazahstantsev-mogut-arestovat-chujie-kommentarii-ih-282818/> accessed 7 July 2019

Akhal-Tech Collective, ‘Kyrgyzstan Blocks Archive.Org on “Extremism” Grounds’ (*Global Voices*, 21 July 2017) <https://globalvoices.org/2017/07/21/kyrgyzstan-blocks-archive-org-on-extremism-grounds/> accessed 22 June 2019

Alekseyev M, ‘Konets Svyazi. Novyy Zakon Zastavit Operatorov Otklyuchit’ Anonimnyye Sim-Karty [The End of Communication. New Bill Obliged Mobile Operators to Disconnect Anonymous SIM-Cards]’ (*Forbes.ru*, 13 April 2018) <https://www.forbes.ru/tehnologii/360093-konec-svyazi-novyy-zakon-zastavit-operatorov-otklyuchit-anonimnye-sim-karty> accessed 30 July 2019

‘AliExpress to Open Representation in Russia and Comply with Personal Data Storage Law’ (*East-West Digital News*, 21 March 2017) <https://www.ewdn.com/2017/03/21/aliexpress-to-

open-representation-in-russia-and-comply-with-personal-data-storage-law/> accessed 4 July 2019

Anderson N, 'Russia, China, Tajikistan Propose UN "Code of Conduct" for the 'Net' (*Ars Technica*, 20 September 2011) <https://arstechnica.com/tech-policy/news/2011/09/russia-china-tajikistan-propose-un-code-of-conduct-for-the-net.ars> accessed 18 August 2019

Anischchuk A, 'Putin Admits Russian Forces Were Deployed to Crimea' *Reuters* (17 April 2014) <https://www.reuters.com/article/russia-putin-crimea-idUSL6N0N921H20140417> accessed 12 September 2019

'Announcement of the Central Commission of the Republic of Belarus on Elections and the Conduct of Republican Referenda on the Results of the Republican Referendum on October 17, 2004 (Archieved)' (23 October 2006) <https://web.archive.org/web/20061023120330/http://rec.gov.by/refer/refer2004result.html#> accessed 26 June 2019

'Announcement of the Kazkahstani Association of IT Companies' (8 June 2011) <https://nic.kz/docs/announc_14_06_2011.jsp> accessed 4 July 2019

Aoki K, 'How to Hide Your Identity and Data on the Web With a VPN' (*Lifewire*, 14 October 2016) <https://www.lifewire.com/what-is-a-vpn-2377977> accessed 3 August 2019

'Apple Provides Details on Compliance with Russian Data-Localization Law' (*East-West Digital News*, 5 February 2019) <https://www.ewdn.com/2019/02/05/apple-provides-russian-authorities-with-details-on-compliance-with-data-localization-law/> accessed 4 July 2019

Arykbaev E, 'Sud v Kyrgyzstane priznal ekstremistskim muzykal'nyy servis SoundCloud [Court in Kyrgyzstan cognized SoundCloud music service as extremist]' (*KLOOP.KG*, 11 May 2018) <https://kloop.kg/blog/2018/05/11/sud-v-kyrgyzstane-priznal-ekstremistskim-

muzykalnyj-servis-soundcloud/> accessed 22 June 2019

Asipov M, 'Kto Blokiruyet Neugodnyye Sayty v Kaznete [Who Blocks Unwanted Websites in Kaznet? Archieved]' (*Esquire*, 28 September 2015) <https://web.archive.org/web/20170402082300/https://www.esquire.kz/3128-kto_blokiruet_neugodnie_sayti_v_kaznete> accessed 4 July 2019

Auyezov O, 'Kazakhstan's Leader Nazarbayev Resigns after Three Decades in Power' *Reuters* (20 March 2019) <https://www.reuters.com/article/us-kazakhstan-president-idUSKCN1R01N1> accessed 25 June 2019

Azhigaliev M, 'Skol'ko kazakhstantsev osudili za rasprostraneniye lozhnoy informatsii v Internete [How many Kazakhstanis have been convicted for spreading false information on the Internet]' (*Tengrinews.kz*, 15 January 2018) <https://tengrinews.kz/internet/skolko-kazahstantsev-osudili-rasprostranenie-lojnoy-335392/> accessed 20 June 2019

'Background on Nursultan Nazarbayev' (*Carnegie Endowment for International Peace*, 26 March 2012) <https://carnegieendowment.org/2012/03/26/background-on-nursultan-nazarbayev-pub-47648> accessed 25 June 2019

Baidildayeva D, 'Internet Censorship in Kazakhstan: More Pervasive than You May Think' (*openDemocracy*, 26 March 2018) <https://www.opendemocracy.net/en/odr/internet-censorship-in-kazakhstan/> accessed 21 July 2019

Bailey R, 'I Learned It By Watching You!' (2016) 48 Reason <https://reason.com/2016/11/01/i-learned-it-by-watching-you/> accessed 4 October 2019

Baird L, 'Russia to Increase Data Audits in 2016 With Data Localization Law & More News on The EU's Safe Harbor Ruling' (*Life Sciences Legal Update*, 8 January 2016) <https://www.lifescienceslegalupdate.com/2016/01/articles/industry-developments/russia-to-

increase-data-audits-in-2016-with-data-localization-law-more-news-on-the-eus-safe-harbor-ruling/> accessed 4 July 2019

Barlow JP, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 8 February 1996) <https://www.eff.org/cyberspace-independence> accessed 14 September 2019

Bastunets A, 'Analysis of Amendments to Media Law' (*BAJ*, 22 January 2015) <http://old.baj.by/be/node/27559> accessed 22 June 2019

Bayram M, 'UZBEKISTAN: Harshened Criminal and Administrative Code Punishments' (*Forum 18*, 15 June 2016) <http://www.forum18.org/archive.php?article_id=2189> accessed 14 September 2019

'Beirut Wants "terrorism" Defined' (*Aljazeera*, 13 January 2004) <https://www.aljazeera.com/archive/2004/01/200841010738460226.html> accessed 18 July 2019

'Belarus — The World Factbook' (*Central Intelligence Agency*) <https://www.cia.gov/library/publications/the-world-factbook/geos/bo.html#Govt> accessed 25 June 2019

'Belarus Adopts Restrictive Media Law Amendments, Blocks Websites' (*Committee to Protect Journalists*, 23 December 2014) <https://cpj.org/2014/12/belarus-adopts-restrictive-media-law-amendments-bl.php> accessed 14 September 2019

'Belarus: Open Joint NGO Letter to the Parliament of Belarus' (*Human Rights Watch*, 20 October 2011) <https://www.hrw.org/news/2011/10/20/belarus-open-joint-ngo-letter-parliament-belarus> accessed 23 June 2019

‘Belarus Passes Legislation Against “Fake News” Media’ (*RadioFreeEurope/RadioLiberty*, 14 June 2018) <https://www.rferl.org/a/belarus-assembly-passes-controversial-fake-news-media-legislation/29291033.html> accessed 20 June 2019

‘Belarus Rolls Out Big Brother to Counter Worst Unrest in Decades’ (27 March 2017) <https://www.bloomberg.com/news/articles/2017-03-27/belarus-rolls-out-big-brother-to-counter-worst-unrest-in-decades> accessed 7 July 2019

‘Belarusian Authorities Want to Completely Block Independent Websites’ (*Charter 97*, 2015) <https://charter97.org/en/news/2015/2/25/140908/> accessed 21 June 2019

‘Belarus’s Lukashenko: “Better a Dictator than Gay”’ *Reuters* (4 March 2012) <https://www.reuters.com/article/us-belarus-dicator-idUSTRE8230T320120304> accessed 25 June 2019

‘Bill On Autonomous Operation Of Russia’s Internet Submitted To Duma’ (*RadioFreeEurope/RadioLiberty*, 14 December 2018) <https://www.rferl.org/a/bill-on-autonomous-operation-of-russia-s-internet-submitted-to-duma/29656655.html> accessed 5 July 2019

‘Blocking of Leading Belarusian News Website Seen as Test for EU’ (*RSF*, 30 January 2018) <https://rsf.org/en/news/blocking-leading-belarusian-news-website-seen-test-eu> accessed 25 June 2019

‘«Blokirovka ZHZH»: prichina «v provayderakh Kazakhstana», govoryat spetsialisty [“LJ blocking”: the reason is “in the providers of Kazakhstan,” experts say]’ (*KLOOP.KG*, 10 October 2008) <https://kloop.kg/blog/2008/10/10/blokirovka-zhzh-prichina-v-provajderax-kazaxstana-govoryat-specialisty/> accessed 22 June 2019

Blome N and Diekmann K, ‘For Me, It Is Not Borders That Matter’ (*Bild*, 2016)

<https://www.bild.de/politik/ausland/wladimir-putin/russian-president-vladimir-putin-the-interview-44092656.bild.html> accessed 12 September 2019

'Boleye 30 tys. saytov za god blokiruyetsya v Kazakhstane [More than 30 thousand sites during that year are blocked in Kazakhstan]' (*Digital Report*, 8 June 2017) <https://digital.report/bolee-30-tyis-saytov-za-god-blokiruetsya-v-kazahstane/> accessed 14 September 2019

Bryzgalova E and Boletskaya K, 'Roskomnadzor reshil poka ne blokirovat' VPN-servisy [Roskomnadzor decided not to block VPN services yet]' (*Vedomosti*, 26 June 2019) <https://www.vedomosti.ru/technology/articles/2019/06/26/805110-roskomnadzor> accessed 26 July 2019

Budnitsky S, 'Digital Eurasia: Big brother in Eurasia' (*Digital Report*, 13 November 2014) <https://digital.report/digital-eurasia-big-brother-eurasia/> accessed 5 July 2019

Burdin V, 'Gossluzhashchim RK zapretili kritikovat' vlast' v sotssetyakh [State officials not allowed to criticize the power]' (*Forbes.kz*, 12 January 2015) <https://forbes.kz//process/internet/gosslujaschim_i_byudjetnikam_rk_zapretili_kritikovat_vlast_v_sotssetyah/> accessed 20 June 2019

'Bush Welcomes New Nato Members' (*BBC*, 29 March 2004) <http://news.bbc.co.uk/2/hi/europe/3578837.stm> accessed 11 March 2020

Bykovsky P, 'Belarus': blokirovka anonimayzerov v Baynete [Belarus: blocking anonymizers in Bynet]' (*DW.COM*, 25 February 2015) <https://bit.ly/2RAgFdN> accessed 24 June 2019

——, 'Kak v Belarusi oboyti blokirovku Tor i izbezhat' tsenzury [How to overcome Tor blocking in Belarus and avoid censorship]' (*DW.COM*, 5 December 2016)

<https://bit.ly/2FxLX0g> accessed 24 June 2019

——, ‘Belarus’ ne budet trebovat’ khraneniya personal’nykh dannykh v strane [Belarus will not require the storage of personal data in the country]’ (*DW.COM*, 13 June 2019) <https://bit.ly/2RRVW5v> accessed 4 July 2019

Cadwalladr C and Graham-Harrison E, ‘Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach’ *The Guardian* (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 14 June 2019

Carlson K, ‘Armenian Bill Threatens Online Anonymity’ (*Electronic Frontier Foundation*, 16 April 2014) <https://www.eff.org/deeplinks/2014/04/armenian-bill-threatens-online-anonymity> accessed 6 July 2019

Carr J, ‘4 Problems with China and Russia’s International Code of Conduct for Information Security’ (*Digital Dao*, 22 September 2011) <http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html> accessed 18 August 2019

Cellan-Jones R, ‘Russia “Meddled in All Big Social Media”’ *BBC News* (17 December 2018) <https://www.bbc.com/news/technology-46590890> accessed 18 August 2019

‘Censorship by Country: Kazakhstan.’ (*Torproject*, 2017) <https://trac.torproject.org/projects/tor/wiki/doc/OONI/censorshipwiki/CensorshipByCountry/Kazakhstan#a20348> accessed 24 June 2019

‘Changes to the Open Internet in Kazakhstan’ (*Official Google Blog*, 7 June 2011) <https://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html> accessed 4 July 2019

Chevtaeva I, 'Blokirovka LinkedIn v Rossii Priznana Zakonnoy [LinkedIn Ban in Russia Is Recognized as Legal]' (*Vedomosti*, 10 October 2016) <https://www.vedomosti.ru/technology/articles/2016/11/10/664394-blokirovka-linkedin> accessed 4 July 2019

Chimiris E, 'Eastern Partnership Countries: Buffer Zone or Platform for Dialogue?' (*Modern Diplomacy*, 13 November 2019) <https://moderndiplomacy.eu/2019/11/13/eastern-partnership-countries-buffer-zone-or-platform-for-dialogue/> accessed 11 March 2020

Chizhova L, Mayetnaya Y and Coalson R, 'Only A Few "Likes" For Putin's Softening Of Controversial Meme Law' (*Radio Free Europe/Radio Liberty*, 2018) <https://www.rferl.org/a/russia-putin-meme-laws-softening-critics-stifling-dissent-freedom-speech/29527682.html> accessed 14 September 2019

Chkheidze T, 'Internet Control in Georgia' (*HUMANRIGHTS.GE*, 17 November 2010) <http://www.humanrights.ge/index.php?a=main&pid=12564&lang=eng> accessed 2 July 2019

Chubrik A, *Russia: The Belarusian Challenge* (Carnegie Moscow Center 2016) <https://carnegieendowment.org/files/6.pdf> accessed 5 July 2019

'Commentary to Decree No. 187 of 25 May 2017' (*Official Internet Portal of the President of the Republic of Belarus*, 26 May 2017) <http://president.gov.by/en/news_en/view/commentary-to-decree-no-187-of-25-may-2017-16293/> accessed 7 July 2019

Commonwealth of Independent States, 'Free Trade Agreement between Azerbaijan, Armenia, Belarus, Georgia, Moldova, Kazakhstan, the Russian Federation, Ukraine, Uzbekistan, Tajikistan and the Kyrgyz Republic (Translation)' (*WIPO Lex*, 15 April 1994)

<https://wipolex.wipo.int/en/text/228813> accessed 12 September 2019

Corley F, 'Kazakhstan: Article 174 Cases Increase, Cancer Sufferer Tortured' (Forum 18 2017) <https://www.refworld.org/docid/58bfbe4c4.html> accessed 14 September 2019

'Data Retention across the EU' (*European Union Agency for Fundamental Rights*, 16 December 2015) <https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention> accessed 17 September 2019

'Defamation Law and Practice in Belarus, Moldova and Ukraine' (*Article 19 – Global Campaign for free expression,* 2006) <https://www.refworld.org/pdfid/4756cfef0.pdf> accessed 18 September 2019

Dennis MA, 'Wiki: Web Site' (*Encyclopedia Britannica*) <https://www.britannica.com/topic/wiki> accessed 21 July 2019

Désir H, 'Blocking of News Website and Detention of Journalists in Kazakhstan of Grave Concern, Says OSCE Representative on Freedom of the Media' (*OSCE*, 5 April 2018) <https://www.osce.org/representative-on-freedom-of-media/376966> accessed 20 June 2019

——, 'Legislative Amendments Further Restrict Media in Belarus, Says OSCE Media Freedom Representative' (*OSCE*) <https://www.osce.org/representative-on-freedom-of-media/384786> accessed 27 June 2019

'Dictionary by Merriam-Webster' <https://www.merriam-webster.com/> accessed 14 August 2019

Digital Security Lab, 'Legal Analysis of the Draft Law "On Amending Certain Laws of Ukraine on Countering Threats to National Security in Information Sector," Registration #6688' (*Medium*, 2 July 2018) <https://medium.com/@cyberlabukraine/legal-analysis-of-the-

draft-law-on-amending-certain-laws-of-ukraine-on-countering-threats-to-39b3738d97cf> accessed 22 June 2019

'Disdaining Press Freedom, Kazakhstan Undermines OSCE' (*Committee to Protect Journalists*, 14 September 2010) <https://cpj.org/reports/2010/09/disdaining-press-freedom-kazakhstan-undermines-osc.php> accessed 16 July 2019

'Dostup k LiveJournal vosstanovlen v Kazakhstane [Access to LiveJournal recovered in Kazakhstan]' (*Tengrinews.kz*, 11 November 2015) <https://tengrinews.kz/internet/dostup-k-LiveJournal-vosstanovlen-v-kazahstane-283868/> accessed 21 July 2019

'Education for Justice University Module Series. Defining Terrorism.' (*UNODC*, July 2018) <https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html> accessed 8 August 2019

'Education for Justice University Module Series: Radicalization & Violent Extremism' (*UNODC*, July 2018) <https://www.unodc.org/e4j/en/terrorism/module-2/key-issues/radicalization-violent-extremism.html> accessed 11 August 2019

'Encryption: A Matter of Human Rights' (*Amnesty International,* 2016) https://www.amnestyusa.org/wp-content/uploads/2017/04/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf accessed 23 June 2019

'EU Criticizes Russia's "Foreign Agents" Media Law' (*RadioFreeEurope/RadioLiberty*, 26 November 2017) <https://www.rferl.org/a/russia-putin-signs-foreign-agent-media-law-rferl-voa-cnn-deutsche-welle/28876680.html> accessed 23 June 2019

'EU Member Countries in Brief' (*European Union*, 16 June 2016) <https://europa.eu/european-union/about-eu/countries/member-countries_en> accessed 11 March 2020

‘Eurasia’ (*Freedom House*) <https://freedomhouse.org/regions/eurasia> accessed 25 June 2019

‘European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech’ (*European Commission*, 31 May 2016) <https://europa.eu/rapid/press-release_IP-16-1937_en.htm> accessed 3 August 2019

‘Expert: The Year Was Rather Tense for Armenian Jouranalists’ (*yerkramas.org*, 19 December 2014) <http://yerkramas.org/article/85307/uxodyashhij-god-byl-dlya-armyanskix-zhurnalistov-dostatochno-napryazhennym-%E2%80%93-ekspert> accessed 2 August 2019

‘Facebook i Twitter dali yeshche devyat’ mesyatsev dlya lokalizatsii dannykh rossiyan v RF [Facebook and Twitter were given another nine months to localize Russian data in the Russian Federation]’ (*Interfax.ru*, 16 April 2019) <https://www.interfax.ru/russia/658372> accessed 4 July 2019

‘Fact Sheet - Human Rights in Kazakhstan’ (*Human Rights Watch*, 18 November 2009) <https://www.hrw.org/news/2009/11/18/fact-sheet-human-rights-kazakhstan> accessed 2 July 2019

‘Factsheet: What Is the OSCE?’ (*OSCE*, 11 July 2019) <https://www.osce.org/whatistheosce/factsheet> accessed 7 August 2019

‘“False Information” Laws Must Not Be Used to Silence the Media in Kazakhstan’ (*IFEX*, 18 May 2018) <https://ifex.org/false-information-laws-must-not-be-used-to-silence-the-media-in-kazakhstan/> accessed 16 September 2019

Farrel H, ‘Why the Hidden Internet Can’t Be a Libertarian Paradise’ (*Aeon*, 20 February 2015) <https://aeon.co/essays/why-the-hidden-internet-can-t-be-a-libertarian-paradise> accessed 14 September 2019

‘Fire and Fury for Facebook’ (*Interntational Financial Law Review*, 2018) <https://www.iflr.com/Article/3803223/Fire-and-fury-for-Facebook.html?ArticleId=3803223> accessed 14 September 2019

‘First Amendment’ (*Legal Information Institute*, 6 August 2007) <https://www.law.cornell.edu/wex/first_amendment> accessed 14 August 2019

Fitzpatrick J, ‘What’s the Difference Between a VPN and a Proxy?’ (*How-To Geek*, 18 June 2019) <https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/> accessed 19 August 2019

Foy H and Seddon M, ‘Russian Technology: Can the Kremlin Control the Internet?’ (*Financial Times*, 5 June 2019) <https://www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2> accessed 5 July 2019

‘Freedom in the World 2018’ (*Freedom House*, 13 January 2018) <https://freedomhouse.org/report/freedom-world/freedom-world-2018> accessed 25 June 2019

‘Freedom of Expression Unfiltered: How Blocking and Filtering Affect Free Speech’ (*Article 19 - Global Campaign for free expression*, 2016) <https://www.article19.org/resources/freedom-of-expression-unfiltered-how-blocking-and-filtering-affect-free-speech/> accessed 14 June 2019

‘Freedom on the Net 2011: Kazakhstan’ (*Freedom House*, 13 January 2012) <https://freedomhouse.org/report/freedom-net/2011/kazakhstan> accessed 21 June 2019

‘Freedom on the Net 2012: Belarus’ (*Freedom House*, 17 September 2012) <https://freedomhouse.org/report/freedom-net/2012/belarus> accessed 23 June 2019

‘Freedom on the Net 2012: Kazakhstan’ (*Freedom House*, 18 September 2012) <https://freedomhouse.org/report/freedom-net/2012/kazakhstan> accessed 21 July 2019

‘Freedom on the Net 2014: Kazakhstan’ (*Freedom House*, 26 November 2014) <https://freedomhouse.org/report/freedom-net/2014/kazakhstan> accessed 14 September 2019

‘Freedom on the Net 2015: Armenia’ (*Freedom House*, 27 October 2015) <https://freedomhouse.org/report/freedom-net/2015/armenia> accessed 22 June 2019

‘Freedom on the Net 2015: Belarus’ (*Freedom House*, 27 October 2015) <https://freedomhouse.org/report/freedom-net/2015/belarus> accessed 21 June 2019

‘Freedom on the Net 2016: Azerbaijan’ (*Freedom House*, 10 November 2016) <https://freedomhouse.org/report/freedom-net/2016/azerbaijan> accessed 19 June 2019

‘Freedom on the Net 2016: Georgia’ (*Freedom House*, 9 November 2016) <https://freedomhouse.org/report/freedom-net/2016/georgia> accessed 22 June 2019

‘Freedom on the Net 2016: Kazakhstan’ (*Freedom House*, 10 November 2016) <https://freedomhouse.org/report/freedom-net/2016/kazakhstan> accessed 22 June 2019

‘Freedom on the Net 2017: Azerbaijan’ (*Freedom House*, 14 November 2017) <https://freedomhouse.org/report/freedom-net/2017/azerbaijan> accessed 19 June 2019

‘Freedom on the Net 2017: Russia’ (*Freedom House*) <https://freedomhouse.org/report/freedom-net/2017/russia> accessed 14 September 2019

‘Freedom on the Net 2018: Belarus’ (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/belarus> accessed 25 June 2019

‘Freedom on the Net 2018: Kazakhstan’ (*Freedom House*, 1 November 2018)

<https://freedomhouse.org/report/freedom-net/2018/kazakhstan> accessed 25 June 2019

'Freedom on the Net 2018: Kyrgyzstan' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/kyrgyzstan> accessed 25 June 2019

'Freedom on the Net 2018: Russia' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/russia> accessed 23 June 2019

'Freedom on the Net 2018: The Rise of Digital Authoritarianism' (*Freedom House*, 30 October 2018) <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism> accessed 5 September 2019

'Freedom on the Net 2018: Ukraine' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/ukraine> accessed 14 September 2019

'Freedom on the Net 2018: Uzbekistan' (*Freedom House*, 1 November 2018) <https://freedomhouse.org/report/freedom-net/2018/uzbekistan> accessed 25 June 2019

Gavron A, 'Minskiye sledovateli obzavelis' kompleksom po izvlecheniyu dannykh iz smartfonov [Minsk investigators acquired a complex to extract data from smartphones]' (*Minsk News*, 22 July 2016) <https://minsknews.by/minskie-sledovateli-obzavelis-kompleksom-po-izvlecheniyu-dannyih-iz-smartfonov/> accessed 7 July 2019

Gershkovich E, 'Will Russia Stop Arresting Its Citizens For Posting Memes?' (*The Moscow Times*, 4 October 2018) <https://www.themoscowtimes.com/2018/10/04/will-russia-stop-arresting-citizens-for-memes-a63090> accessed 14 September 2019

Geybulla A, 'Azerbaijan's Blocking of Websites Is a Sign of Further Restrictions Online' (*openDemocracy*, 31 August 2018) <https://www.opendemocracy.net/en/odr/azerbaijans-blocking-of-websites/> accessed 22 June 2019

Gishyan R, ‘Datarany Masnakioren Bavararets’ Vostikanut’yan Hayts’n Ynddem SOS TV-i [The Court Partially Satisfied the Lawsuit Filed by the Police against SOS TV]’ (*Radio Free Europe/Radio Liberty Armenian Service*, 14 March 2017) <https://www.azatutyun.am/a/28368592.html> accessed 19 June 2019

Gladwell M, ‘Does Egypt Need Twitter?’ <https://www.newyorker.com/news/news-desk/does-egypt-need-twitter> accessed 20 August 2019

‘Google.Kz Vernulsya v Kazakhstan [Google.Kz Returned to Kazakhstan Google.Kz]’ (*Tengrinews*, 15 June 2011) <https://tengrinews.kz/internet/Googlekz-vernulsya-v-kazahstan-190571/> accessed 4 July 2019

Griffiths J, ‘China Is Exporting the Great Firewall as Internet Freedom Declines around the World’ (*CNN*, 2 November 2018) <https://www.cnn.com/2018/11/01/asia/internet-freedom-china-censorship-intl/index.html> accessed 9 July 2019

Grytsenko O, ‘Thousands of Russian Soldiers Fought at Ilovaisk, around a Hundred Were Killed’ (*KyivPost*, 6 April 2018) <https://www.kyivpost.com/thousands-russian-soldiers-fought-ilovaisk-around-hundred-killed> accessed 12 September 2019

——, ‘Parliament Committee Okays Bill Critics Say Will Block Websites, End Internet Anonymity’ (*KyivPost*, 5 July 2018) <https://www.kyivpost.com/ukraine-politics/parliament-committee-okays-bill-critics-say-will-block-websites-end-internet-anonymity.html> accessed 22 June 2019

Harding L, ‘Russia Delegation Suspended from Council of Europe over Crimea’ (2014) <https://www.theguardian.com/world/2014/apr/10/russia-suspended-council-europe-crimea-ukraine> accessed 12 September 2019

Hern A, ‘Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes,

Documents Claim' *The Guardian* (6 July 2015) <https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim> accessed 7 July 2019

'Human Rights in Kazakhstan: Seven Months before the OSCE Chairmanship' (*Human Rights Watch*, 20 May 2009) <https://www.hrw.org/news/2009/05/20/human-rights-kazakhstan-seven-months-osce-chairmanship> accessed 22 June 2019

Hunter R and Heinke D, 'Perspective: Radicalization of Islamist Terrorists in the Western World' (*FBI: Law Enforcement Bulletin*, 1 September 2011) <https://leb.fbi.gov/articles/perspective/perspective-radicalization-of-islamist-terrorists-in-the-western-world> accessed 10 August 2019

'IMEI –Codes Registration System to Be Applied in Azerbaijan' (*News.Az*, 15 March 2013) <https://news.az/articles/tech/77977> accessed 26 June 2019

'Independent News Website Partly Blocked In Kyrgyzstan' (*RadioFreeEurope/RadioLiberty*, 22 February 2012) <https://www.rferl.org/a/independent_news_website_partly_blocked_in_kyrgyzstan/24492408.html> accessed 25 June 2019

INFORM.KZ, 'Zakon o Lidere Natsii opublikovan v ofitsial'noy presse respubliki [Law on the Leader of the Nation published in the official press of the republic]' (*INFORM.KZ*, 15 June 2010) <https://www.inform.kz/ru/article/2278166> accessed 19 June 2019

Ingram M, 'Was What Happened in Tunisia a Twitter Revolution?' (*Gigaom*, 14 January 2011) <https://gigaom.com/2011/01/14/was-what-happened-in-tunisia-a-twitter-revolution/> accessed 20 August 2019

'Insights into Internet Freedom in Central Asia: Belarus' (*Digital Defenders Partnership*)

<https://www.digitaldefenders.org/belarus/> accessed 5 July 2019

'Instruction on the Procedure for Interaction of Telecommunication Operators and Mobile Cellular Operators with State Bodies of the Kyrgyz Republic Engaged in Operational

'Internet Distributor Registery' (*Roskomnadzor*) <https://97-fz.rkn.gov.ru/> accessed 28 June 2019

'Internet Intermediaries: Dilemma of Liability' (*Article 19- Global Campaign for free expression*, 20 August 2013) <https://www.article19.org/resources/internet-intermediaries-dilemma-liability/> accessed 3 September 2019

'Internet Society Perspectives on Internet Content Blocking: An Overview' (*Internet Society*, March 2017) <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/> accessed 19 August 2019

'Internet Users' Rights' (*Council of Europe/Conseil de l'Europe*, 16 April 2014) <https://www.coe.int/en/web/freedom-expression/internet-users-rights> accessed 3 August 2019

'Interv'yu Negosudarstvennym Sredstvam Massovoy Informatsii [Interview for Non-State Media]' (*Official website of the President of the Republic of Belarus*, 2015) <http://president.gov.by/ru/news_ru/view/intervjju-negosudarstvennym-sredstvam-massovoj-informatsii-11882/> accessed 12 September 2019

Isayev T, 'V Uzbekistane registratsiya mobil'nykh telefonov po IMEI budet besplatnoy [IMEI Registration of Mobile Devices will be Free of Charge in Uzbekistan]' (*Podrobno.uz*, 30 March 2019) <https://podrobno.uz:443/cat/tehnp/v-uzbekistane-registratsiya-/> accessed 1 August 2019

‘Joint Declaration on Media Independence and Diversity in the Digital Age’ (*OSCE*, 2 May 2018) <https://www.osce.org/representative-on-freedom-of-media/379351> accessed 14 September 2019

Karpenko O, ‘V Ukraine takzhe mogut vvesti reyestr zapreshchennykh saytov [Ukraine may introsuce the register of prohibited sites]’ (*AIN.UA*, 6 November 2012) <https://ain.ua/2012/11/06/v-ukraine-takzhe-mogut-vvesti-reestr-zapreshhennyx-sajtov/> accessed 21 June 2019

——, ‘Prezident zablokiroval «Yandeks» v Ukraine yeshche na tri goda. I ryad drugikh IT-kompaniy [The president blocked Yandex in Ukraine for another three years. And a number of other IT companies]’ (*AIN.UA*, 20 March 2019) <https://ain.ua/2019/03/20/opyat-blokiruetsya-yandeks-v-ukraine/> accessed 21 June 2019

‘Kazakhstan’ (*Human Rights Watch*) <https://www.hrw.org/europe/central-asia/kazakhstan> accessed 25 June 2019

‘Kazakhstan: Criminal Probe of Media Outlets’ (*Human Rights Watch*, 6 April 2018) <https://www.hrw.org/news/2018/04/06/kazakhstan-criminal-probe-media-outlets> accessed 20 June 2019

‘Kazakhstan: S 1 iyulya 2017 goda operatory budut blokirovat’ nezaregistrirovannyye telefony [Kazakhstan: From July 1, 2017, operators will block unregistered phones]’ (*Digital Report*, 25 January 2017) <https://digital.report/kazahstan-s-1-iyulya-2017-goda-operatoryi-budut-blokirovat-nezaregistrirovannyie-telefonyi/> accessed 27 June 2019

‘Kazakhstan Should Drop “False Information” Case against Critical Media Outlets’ (*International Press Institute*, 13 April 2018) <https://ipi.media/kazakhstan-should-drop-false-information-case-against-critical-media-outlets/> accessed 20 June 2019

‘Kazakhstan Shuts Down Independent News Site’ (*RadioFreeEurope/RadioLiberty*, 2018) <https://www.rferl.org/a/kazakhstan-shuts-down-independent-news-site-ratel/29254964.html> accessed 16 September 2019

‘Kazakhstan: Strikes, Arrests and Fears of New Restrictions on Fundamental Freedoms’ (*CIVICUS*, 31 January 2018) <https://monitor.civicus.org/newsfeed/2018/01/31/kazakhstan-strikes-arrests-and-fears-new-restrictions-fundamental-freedoms/> accessed 25 June 2019

Kemp S, ‘Digital 2019: Global Internet Use Accelerates’ (*We Are Social*, 30 January 2019) <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates> accessed 18 July 2019

‘Komissiya Parlamenta Armenii Reshila «otlozhit’ v Dolgiy Yashchik» Skandal’nyy Zakonoproyekt Protiv «feykov» [The Parliamentary Commission Indefinetely Posponed Unfamous Fake News Bill]’ (*Panorama.am*, 25 April 2014) <https://www.panorama.am/ru/news/2014/04/25/a-bill-about-press/301560> accessed 2 August 2019

Koval I, ‘God zakonu ob anonimayzerakh i VPN: kak im zhivetsya v Rossii? [Year to the law on anonymizers and VPN: how do they live in Russia?]’ (*DW.COM*, 30 July 2018) <https://bit.ly/2M0KFfv> accessed 24 June 2019

Kravchenko M, ‘Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2014’ (*SOVA Center*, 2015) <http://www.sova-center.ru/en/misuse/reports-analyses/2015/06/d32083> accessed 14 September 2019

——, ‘Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2016’ (*SOVA Center*, 2017) <http://www.sova-center.ru/en/misuse/reports-analyses/2017/04/d36857> accessed 14 September 2019

‘Krym i Rossiya: porozn’ ili vmeste? [Crimea and Russia: apart or together?]’ (*WCIOM*, 2014) <https://wciom.ru/index.php?id=236&uid=855> accessed 12 September 2019

Kucera J, ‘CSTO Fires Salvo in Information War’ (*Eurasianet*, 27 December 2010) <https://eurasianet.org/csto-fires-salvo-in-information-war> accessed 18 August 2019

——, ‘With Eye To Arab Spring, CSTO Strengthens Cyber, Military Powers’ (*Eurasianet*, 15 August 2011) <https://eurasianet.org/with-eye-to-arab-spring-csto-strengthens-cyber-military-powers> accessed 18 August 2019

——, ‘Russian Press Portrays Armenia’s Pashinyan as “Carbon Copy” of Poroshenko’ (*Eurasianet*, 23 July 2018) <https://eurasianet.org/russian-press-portrays-armenias-pashinyan-as-carbon-copy-of-poroshenko> accessed 12 September 2019

——, ‘Pashinyan Takes on “Fake News”’ (*Eurasianet*, 9 April 2019) <https://eurasianet.org/pashinyan-takes-on-fake-news> accessed 27 August 2019

Kumenov A, ‘Kazakhstan: Online Anonymity Ban in Force from April’ (*Eurasianet*, 2 February 2018) <https://eurasianet.org/kazakhstan-online-anonymity-ban-in-force-from-april> accessed 27 June 2019

‘Kyrgyzstan Censors Leading News Agency Ferghana’ (*IFEX*, 14 June 2017) <https://ifex.org/kyrgyzstan-censors-leading-news-agency-ferghana/> accessed 25 June 2019

‘Kyrgyzstan: Growing Pressure on Media Groups’ (*Human Rights Watch*, 27 March 2017) <https://www.hrw.org/news/2017/03/27/kyrgyzstan-growing-pressure-media-groups> accessed 19 June 2019

‘Kyrgyzstan Holds Three Trials in One Day against Independent Outlet’ (*Committee to Protect Journalists*, 29 June 2019) <https://cpj.org/2017/06/kyrgyzstan-holds-three-trials-in-

one-day-against-i.php> accessed 19 June 2019

'Kyrgyzstan: Human Rights Defenders, Independent Media Targeted in Defamation Case' (*Freedom House*, 2 May 2017) <https://freedomhouse.org/article/kyrgyzstan-human-rights-defenders-independent-media-targeted-defamation-case> accessed 19 June 2019

'Kyrgyzstan: Law on Countering Extremist Activity' (*Article 19 - Global Campaign for free expression,* 2015) <https://www.article19.org/data/files/medialibrary/38221/Kyrgyzstan-Extremism-LA-Final.pdf> accessed 25 June 2019

'Kyrgyzstan: Stop Legislative Harassment of Zanoza.Kg and Its Journalists' (*Article 19 - Global Campaign for free expression*, 12 August 2017) <https://www.article19.org/resources/kyrgyzstan-stop-legislative-harassment-of-zanoza-kg-and-its-journalists/> accessed 19 June 2019

Lapidus GW, 'Ethnic Conflict in the Former Soviet Union' (*CISAC*, 2005) <https://cisac.fsi.stanford.edu/research/ethnic_conflict_in_the_former_soviet_union/> accessed 13 March 2020

Laukkonen J, 'What a Domain Name Is and How It Works' (*Lifewire*, 12 August 2019) <https://www.lifewire.com/what-is-a-domain-name-2483189> accessed 19 August 2019

Leiva-Gomez M, 'Everything You Should Know About Your IMEI Number' (*Make Tech Easier*, 6 August 2018) <https://www.maketecheasier.com/imei-number/> accessed 31 July 2019

Lillis J, 'Kazakhstan: Terrorist Plot — or Concocted Conspiracy?' (*Eurasianet*, 2 February 2018) <https://eurasianet.org/kazakhstan-terrorist-plot-or-concocted-conspiracy> accessed 25 June 2019

Lokot T, ‘Self-Proclaimed “Donetsk People’s Republic” Now Has an Internet Blacklist’ (*Global Voices*, 17 June 2015) <https://globalvoices.org/2015/06/17/self-proclaimed-donetsk-peoples-republic-now-has-an-internet-blacklist/> accessed 21 June 2019

——, ‘Ukraine’s New Banned Websites Registry: Security Measure or Censorship Tool?’ (*Global Voices*, 22 October 2015) <https://globalvoices.org/2015/10/22/ukraines-new-banned-websites-registry-security-measure-or-censorship-tool/> accessed 21 June 2019

——, ‘Russia’s Internet Watchdog May Soon Get More Extrajudicial Website Blocking Powers’ (*Global Voices Advocacy*, 11 November 2015) <https://advox.globalvoices.org/2015/11/11/russias-internet-watchdog-may-soon-get-more-extrajudicial-website-blocking-powers/> accessed 21 July 2019

——, ‘Ukrainian Separatists Block 100+ News Websites in “Lugansk People’s Republic”’ (*Global Voices*, 14 January 2016) <https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/> accessed 11 July 2019

MacFarquhar N, ‘Russia Quietly Tightens Reins on Web With “Bloggers Law” - The New York Times’ (*New York Times*, 5 June 2014) <https://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html?_r=0> accessed 2 July 2019

Makhovsky A, ‘Belarus Aims to Cut Russian Oil Supplies to 30-40% of Its Requirements: Belta’ *Reuters* (21 January 2020) <https://www.reuters.com/article/us-belarus-oil-russia-diversification-idUSKBN1ZK1ED> accessed 11 March 2020

Maksimova D, ‘Zakonna li proslushka abonentov sotovykh operatorov RK? [Is wiretapping of subscribers of RK by mobile operators legal?]’ (*Kursiv*) <https://kursiv.kz/news/vlast-i-biznes/2017-05/zakonna-li-proslushka-abonentov-sotovykh-operatorov-rk> accessed 20

September 2019

'Manila Principles on Intermediary Liability' (A Global Civil Society Initiative 2015) <https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf> accessed 8 July 2019

Marczak B and others, 'Mapping Hacking Team's "Untraceable" Spyware' (*The Citizen Lab*, 17 February 2014) <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/> accessed 7 July 2019

Martirosyan S, 'Armenia Subject to Censorship from Russia' (*Media.am*, 25 December 2012) <https://media.am/en/blocked-website-in-armenia> accessed 22 June 2019

——, 'Ej.Ru and Bet365.Com Blocked by Russian Roskomnadzor in Armenia' (*Banman.am*, 3 July 2015) <https://www.banman.am/2015/07/ejru-and-bet365com-blocked-by-russian.html> accessed 22 June 2019

Mason R, Syal R and Harding L, 'Azerbaijan Hits Back over "scandalous" Money Laundering Claims' *The Guardian* (5 September 2017) <https://www.theguardian.com/world/2017/sep/05/theresa-may-challenged-over-azerbaijani-money-laundering-scheme> accessed 22 June 2019

'Mass Media in Belarus: E-Newstseller' (BAJ 2014) <https://baj.by/sites/default/files/analytics/files/3372014_mass_media_in_belarus_en.pdf>

'Mass Media Week in Belarus' <https://baj.by/sites/default/files/analytics/files/11-24_08_2014en.pdf> accessed 14 September 2019

Matthews O, 'Russia's Greatest Weapon May Be Its Hackers' (*Newsweek*, 7 May 2015) <https://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html> accessed 12 September 2019

Mayer J, 'How Russia Helped Swing the Election for Trump' <https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump> accessed 18 August 2019

Mearsheimer JJ, 'Getting Ukraine Wrong' *The New York Times* (13 March 2014) <https://www.nytimes.com/2014/03/14/opinion/getting-ukraine-wrong.html> accessed 11 March 2020

'Meeting with Bishops' Council members' (*Website of the President of Russia*) <http://kremlin.ru/events/president/news/17409> accessed 12 September 2019

'Messaging App Viber Reportedly Bows to Russian Data-Localization Law, Relocates User Data to New Servers' (*Meduza*, 19 October 2015) <https://meduza.io/en/news/2015/10/19/messaging-app-viber-reportedly-bows-to-russian-data-localization-law-relocates-user-data-to-new-servers> accessed 4 July 2019

Mielnikiewicz J, 'Post-Crimea, Phantom of Armenian Separatism Haunts Georgia' (*Eurasianet*, 2014) <https://eurasianet.org/post-crimea-phantom-of-armenian-separatism-haunts-georgia> accessed 13 March 2020

Mijatović D, 'New Restrictions in Uzbekistan Further Limit Free Expression on Internet, OSCE Representative Says' (*OSCE*, 8 September 2014) <https://www.osce.org/fom/123275> accessed 19 July 2019

'Ministry of Information Admits That Tor Is Locked in Belarus' (*euroradio.fm*, 7 December 2016) <https://euroradio.fm/en/ministry-information-admits-tor-locked-belarus> accessed 24 June 2019

'Misuse of Anti-Terror Legislation Threatens Freedom of Expression' (*The Council of Europe Commissioner for Human Rights*, 12 April 2018)

<https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/misuse-of-anti-terror-legislation-threatens-freedom-of-expression> accessed 14 September 2019

'Mobile Devices Registration System' (*Ministry of Transport, Communications and High Technologies*) <https://rabita.az/en/c-projects/mdrsen/> accessed 26 June 2019

Morris K, 'Freedom of the Media under Attack across the Former Soviet Union' (*The Foreign Policy Centre*, 24 May 2016) <https://fpc.org.uk/freedom-media-attack-across-former-soviet-union/> accessed 10 July 2019

'Most CIS Countries Sign Up To Free-Trade Zone' (*RadioFreeEurope/RadioLiberty*) <https://www.rferl.org/a/cis_putin_free-trade_zone/24364420.html> accessed 12 September 2019

Muižnieks N, 'Arbitrary Internet Blocking Jeopardises Freedom of Expression' (*Commissioner for Human Rights*, 26 September 2017) <https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/arbitrary-internet-blocking-jeopardises-freedom-of-expression> accessed 10 July 2019

Mushohwe K, 'Everyone Is Now a Journalist, Thanks to the Internet' (*The Herald*) <https://www.herald.co.zw/everyone-is-now-a-journalist-thanks-to-the-internet/> accessed 6 July 2018

'Muted Western Reaction to Putin Poll Win' (19 March 2018) <https://www.bbc.com/news/world-europe-43455950> accessed 25 June 2019

'Nagorno-Karabakh Clashes Kill Dozens' *BBC News* (3 April 2016) <https://www.bbc.com/news/world-europe-35949991> accessed 12 September 2019

‘Nations in Transit 2018: Confronting Illiberalism’ (11 April 2018) <https://freedomhouse.org/report/nations-transit/nations-transit-2018> accessed 30 August 2019

‘Nazarbayev zapretil anonimnyye kommentarii v internete [Nazarbayev Banned Anonymous Comment Online]’ (*NUR.KZ*, 28 December 2017) <https://www.nur.kz/1710097-nazarbaev-zapretil-anonimnye-kommentarii-v-internete.html?> accessed 1 August 2019

Newton, M and Summers J, ‘Russian Data Localization Laws: Enriching “Security” & the Economy’ (*The Henry M. Jackson School of International Studies*, 28 February 2018) <https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/> accessed 4 July 2019

Nikolaichuk A, ‘Moderatory na forumakh v Belarusi vypolnyayut rol’ vakhterov i okhrannikov [Moderators on Belarus forums take the role of watchmen and security guards]’ (*Digital Report*, 27 January 2017) <https://digital.report/moderatoryi-na-forumah-v-belarusi-vyipolnyayut-rol-vahterov-i-ohrannikov/> accessed 6 July 2019

‘Nostal′hiya Za SRSR Ta Stavlennya Do Okremykh Postatey [Nostalgia for the USSR and the Attitude to Individual Figures]’ (*Rating Group*, 2014) <http://ratinggroup.ua/research/ukraine/nostalgiya_po_sssr_i_otnoshenie_k_otdelnym_lichnostyam.html> accessed 12 September 2019

Nurgazinova M, ‘Rabota internet-resursa Vimeo v Kazakhstane vozobnovlena [The work of the Internet resource Vimeo renewed in Kazakhstan]’ (*Kazpravda.kz*, 14 October 2015) <https://www.kazpravda.kz/news/tehnologii/rabota-internet-resursa-vimeo-v-kazahstane-vozobnovlena> accessed 21 July 2019

Nurmakov A, ‘Eksperty: Kazakhstan nameren sledit’ za zashchishchennym trafikom

pol'zovateley [Experts: Kazakhstan intends to monitor the protected traffic of users]' (*Digital Report*, 4 December 2015) <https://digital.report/kz-security-certificate-surveillance/> accessed 7 July 2019

——, 'Siloviki Kazakhstana poluchat polnomochiya po otklyucheniyu svyazi [Security forces of Kazakhstan will be authorized to disable communication]' (*Digital Report*, 14 October 2016) <https://digital.report/siloviki-kazahstana-smogut-otklyuchat-svyazi/> accessed 27 June 2019

'Online Censorship Rounds off Aliyev's Control of Azerbaijani Media' (*RSF*, 3 May 2017) <https://rsf.org/en/news/online-censorship-rounds-aliyevs-control-azerbaijani-media> accessed 22 June 2019

'Opredelen Poryadok Predvaritel'noy Identifikatsii Pol'zovateley Internet-Resursa [The Procedure for Preliminary Identification of Users of the Internet Resource]' (*Pravo.by*, 26 November 2018) <http://www.pravo.by/novosti/novosti-pravo-by/2018/november/31459/> accessed 27 June 2019

'Otmenit' Blokirovku Internet-Resursa Vkontakte [Online Petition: To Cancel Blocking of the Internet Resource Vkontakte]' (*Official online representation of the President of Ukraine*, 29 June 2017) <http://petition.president.gov.ua/petition/36543> accessed 16 July 2019

Pannier B, 'The Victims Of Kazakhstan's Article 174' (*RadioFreeEurope/RadioLiberty*, 2 February 2016) <https://www.rferl.org/a/qishloq-ovozi-kazakhstan-article-174/27527738.html> accessed 14 September 2019

Parks M, 'Brezhnev Son-in-Law to Go on Trial in Corruption Case' (*Los Angeles Times*, 1 July 1988) <https://www.latimes.com/archives/la-xpm-1988-07-01-mn-6406-story.html> accessed 13 March 2020

‘Parlament prinyal zakon, usilivayushchiy kontrol’ nad internet-resursami v Kazakhstane [Parliament passed a law strengthening control over Internet resources in Kazakhstan]’ (*Zakon.kz*, 24 June 2009) <https://www.zakon.kz/141606-parlament-prinjal-zakon-usilivajushhijj.html> accessed 2 July 2019

Petrovskaya G, ‘Belorusskiy segment interneta: pod kolpakom u gosudarstva [Belarusian segment of the Internet: under the hood of the state]’ (*DW.COM*, 24 September 2015) <https://bit.ly/2JwWnhJ> accessed 21 June 2019

‘Po resheniyu suda v Kazakhstane zablokirovan VPN-servis [By a court decision, a VPN service is blocked in Kazakhstan]’ (*Profit.kz*, 12 March 2018) <https://profit.kz/news/45100/Po-resheniu-suda-v-Kazahstane-zablokirovan-VPN-servis/> accessed 24 June 2019

‘Pochti vse uzly Tor v Belarusi zablokirovany. Mogut zablokirovat’ VPN i proksi? [Almost all Tor hosts in Belarus are blocked. Can VPN and proxy be banned?]’ (*euroradio.fm*, 7 December 2016) <https://euroradio.fm/ru/pochti-vse-uzly-tor-v-belarusi-zablokirovanymogut-li-zablokirovat-vpn-i-proksi> accessed 24 July 2019

‘Podpisan Odioznyy Ukaz o Tsenzure Interneta [Odious Decree on Internet Censorship Signed]’ (*Charter 97*, 1 February 2010) <https://charter97.org/ru/news/2010/2/1/25943/> accessed 21 June 2019

‘Podryad na podryadyu: Kakoye slovo nuzhno ubrat’ iz Konstitutsii [Two in a row: What word should be removed from the Constitution]’ (*Novayagazeta.ru*, 17 February 2018) <https://www.novayagazeta.ru/articles/2018/02/17/75540-podryad-na-podryad> accessed 26 June 2019

Polityuk P and Balmforth R, ‘Ukraine Parliament Pushes through Sweeping Anti-Protest

Law' *Reuters* (16 January 2014) <https://www.reuters.com/article/us-ukraine-law-idUSBREA0F12M20140116> accessed 23 June 2019

Pollicino O, 'Legal Analysia of Draft Amendments to the Civil Code of the Republic of Armenia' (Office of the OSCE Representative on Freedom of the Media 2014) <https://www.osce.org/fom/116911?download=true> accessed 7 June 2019

——, 'Fundamental Rights as Bycatch – Russia's Anti-Fake News Legislation' (*Verfassungsblog*, 28 March 2019) <https://verfassungsblog.de/fundamental-rights-as-bycatch-russias-anti-fake-news-legislation/> accessed 17 June 2019

Polovinko V and Sarkisyan L, 'Teper' oni prishli za VPN [Now they came for VPN: Roskomnadzor made the first step to "blocking ways to bypass blacklist"]' (*Novayagazeta.ru*, 28 March 2019) <https://www.novayagazeta.ru/articles/2019/03/28/80032-teper-oni-prishli-za-vpn> accessed 24 June 2019

Poludenko-Young A, 'Ukraine's Security Service Takes Down 30,000 Websites to Fight "Pro-Russian Propaganda"' (*Global Voices*, 28 April 2015) <https://globalvoices.org/2015/04/28/ukraine-censorship-russia-propaganda-hosting/> accessed 22 June 2019

Pomerantsev P, 'Why Europe's Last Dictatorship Keeps Surprising Everyone' *Washington Post* (25 March 2017) <https://www.washingtonpost.com/news/democracy-post/wp/2017/03/25/why-europes-last-dictatorship-keeps-surprising-everyone/> accessed 25 June 2019

'Ponad 30 vlasnykiv ta administratoriv antyukrayins′kykh spil′not u sotsmerezhakh otrymaly vyroky sudu - SBU [More than 30 owners and administrators of anti-Ukrainian communities in social networks received verdicts of the court - the SBU]' (*detector.media*, 28 October

2017) <https://detector.media/infospace/article/131371/2017-10-28-ponad-30-vlasnikiv-ta-administratoriv-antiukrainskikh-spilnot-u-sotsmerezhakh-otrimali-viroki-sudu-sbu/> accessed 14 September 2019

'Popravki v Zakon o SMI: registratsiya internet-izdaniy, identifikatsiya kommentatorov, blokirovka sotssetey [Amendments to the Law on Mass Media: registration of Internet publications, identification of commentators, blocking of social networks]' (*BAJ*, 6 April 2018) <https://baj.by/be/content/popravki-v-zakon-o-smi-registraciya-internet-izdaniy-identifikaciya-kommentatorov-blokirovka> accessed 22 June 2019

Potresov S, '«Popravki Yarovoy i Ozerova», Tsena Voprosa [Amendments by Yarovaya and Ozerov: The Price]' (2016) <https://mobile-review.com/articles/2016/data-storage.shtml> accessed 20 September 2019

'Pravila khraneniya informatsii ob abonentakh operatorami svyazi prinyaty v RK [The rules for storing information about subscribers by telecom operators are taken in the Republic of Kazakhstan]' (*Zakon.kz*, 3 May 2018) <https://www.zakon.kz/4916698-pravila-hraneniya-informatsii-ob.html> accessed 28 June 2019

'Pravitel'stvo utverdilo Kontseptsiyu informatsionnoy bezopasnosti Kyrgyzstana na 2019-2023 gody [The Government approved the Information Security Concept of Kyrgyzstan for 2019-2023]' (*Today.KG*, 17 May 2019) <https://today.kg/news/59446/> accessed 18 August 2019

'Predlozhenija Po Formirovaniju Dolgosrochnoj Programmy Razvitija Rossijskoj Chasti Informacionno-Kommunikacionnoj Seti "Internet" i Svjazannyh s Nej Otraslej Jekonomiki [Suggestions on Formulating the Long-Term Development Programme of the Russian Internet Sector and Related Branches of Economy]'

<http://ири.рф/upload/iblock/2ee/2ee62c7a1204a3717e387869175d81e0.pdf> accessed 14 September 2019

'Press Statement by the Trilateral Contact Group' (*OSCE*, 2014) <https://www.osce.org/home/123124> accessed 12 September 2019

'Priyom po sluchayu tysyacheletiya prestavleniya svyatogo ravnoapostol'nogo knyazya Vladimira [Reception on the occasion of the millennium of Prince St. Vladimir Equal-to-the-Apostles]' (*Website of the President of Russia*) <http://kremlin.ru/events/president/news/50068> accessed 12 September 2019

'Protocol on the Results of Consultations of the Trilateral Contact Group, Signed in Minsk, 5 September 2014' (*OSCE*, 2014) <https://www.osce.org/ru/home/123258> accessed 12 September 2019

'Putin Calls Collapse of Soviet Union "Catastrophe"' (*The Washington Times*, 26 April 2005) <https://www.washingtontimes.com/news/2005/apr/26/20050426-120658-5687r/> accessed 25 June 2019

Putin V, 'Vystupleniye na soveshchanii s poslami i postoyannymi predstavitelyami Rossiyskoy Federatsii [Speech During the Meeting with Ambassadors and Permanent Representatives of the Russian Federation]' (*Official website of the President of Russian Federation*, 2006) <http://kremlin.ru/events/president/transcripts/23669> accessed 9 August 2019

Putz C, 'Karimov, Uzbekistan's Perpetual President' (*The Diplomat*, 11 April 2015) <https://thediplomat.com/2015/04/karimov-uzbekistans-perpetual-president/> accessed 26 June 2019

'Raspredeleniye Blokirovok Saytov Po Vedomstvam [Distribution of Blocking Sites by

Department]' (*Roscomsvoboda*) <https://reestr.rublacklist.net/visual/> accessed 21 June 2019

Rausing S, 'Belarus: Inside Europe's Last Dictatorship' *The Guardian* (7 October 2012) <https://www.theguardian.com/world/2012/oct/07/belarus-inside-europes-last-dictatorship> accessed 25 June 2019

Razumovskaya O, 'Google Moves Some Servers to Russian Data Centers' *Wall Street Journal* (10 April 2015) <https://www.wsj.com/articles/google-moves-some-servers-to-russian-data-centers-1428680491> accessed 4 July 2019

'Recent Legislative Amendments in Uzbekistan Worrying, OSCE Representative Says' (*OSCE*, 29 April 2016) <https://www.osce.org/fom/237641> accessed 14 September 2019

'Recommendation 3/97. Anonymity on the Internet' (Working Party, European Commission 1997) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_en.pdf> accessed 16 June 2019

'Registery of Information Distributors' (*Roskomsvoboda*) <https://reestr.rublacklist.net/distributors_main/> accessed 28 June 2019

Richter A, 'Commentary on the Decree of the President of the Republic of Belarus "On Measures to Improve the Use of the National Segment of the Internet"' (OSCE 2010) <https://www.osce.org/fom/67911?download=true> accessed 10 July 2019

'Robert Legvold on the New Cold War, Interview with Columbia University Professor and Leading Russia Scholar' (*HuffPost*, 11 October 2015) <https://www.huffpost.com/entry/robert-legvold-on-the-new_b_8514120> accessed 12 September 2019

Robinson O, 'The Memes That Might Get You Jailed in Russia' (23 August 2018)

<https://www.bbc.com/news/blogs-trending-45247879> accessed 10 July 2019

Rohozinski R and Haralampieva V, 'Internet Filtering in the Commonwealth of Independent States 2006-2007' (*OpenNet Initiative*, 2007) <https://opennet.net/studies/cis2007> accessed 6 September 2019

'Roskomnadzor zakryl reyestr populyarnykh blogerov [Roskomnadzor Shut Down the Bloggers' Register]' (*NTV*, 1 August 2017) <https://www.ntv.ru/novosti/1880680/?fb> accessed 25 July 2019

Roth A, 'Moscow Court Bans Telegram Messaging App' *The Guardian* (13 April 2018) <https://www.theguardian.com/world/2018/apr/13/moscow-court-bans-telegram-messaging-app> accessed 27 June 2019

——, 'Russia Blocks Millions of IP Addresses in Battle against Telegram App' *The Guardian* (17 April 2018) <https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app> accessed 27 June 2019

——, 'Young Russians Posting Memes Face Jail for "Extremism"' *The Guardian* (1 September 2018) <https://www.theguardian.com/world/2018/sep/01/young-russians-posting-memes-face-jail-for-extremism> accessed 14 September 2019

Rouse M, 'What Is Metadata? - Definition from WhatIs.Com' (*WhatIs.com*, 2014) <https://whatis.techtarget.com/definition/metadata> accessed 19 August 2019

——, 'What Is Deep Packet Inspection (DPI)? - Definition from WhatIs.Com' (*SearchNetworking*, September 2017) <https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI> accessed 19 August 2019

——, ‘What Is a VPN? - Definition from WhatIs.Com’ (*SearchNetworking*, February 2019) <https://searchnetworking.techtarget.com/definition/virtual-private-network> accessed 19 August 2019

——, ‘What Is Encryption? - Definition from WhatIs.Com’ (*SearchSecurity*, May 2019) <https://searchsecurity.techtarget.com/definition/encryption> accessed 19 August 2019

‘Russia: “Big Brother” Law Harms Security, Rights’ (*Human Rights Watch*, 12 July 2016) <https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights> accessed 28 June 2019

‘Russia: EFJ and IFJ Voice Concerns over New Law on Fake News and Respect for State’ (*European Federation of Journalists*, 5 April 2019) <https://europeanjournalists.org/blog/2019/04/05/russia-efj-and-ifj-voice-concerns-over-new-law-on-fake-news-and-respect-for-state/> accessed 20 June 2019

‘Russia, Ukraine Reach Five-Year Gas-Transit Deal’ (*RadioFreeEurope/RadioLiberty*, 2019) <https://www.rferl.org/a/long-russia-ukraine-reach-five-year-gas-transit-deal/30353000.html> accessed 13 March 2020

‘Russian Efforts At Internet Censorship’ (*Radio Free Europe/Radio Liberty*, 13 February 2019) <https://www.rferl.org/a/russian-efforts-at-internet-censorship/29768034.html> accessed 21 June 2019

‘Russian PM Medvedev Says New Cold War Is On’ *BBC News* (13 February 2016) <https://www.bbc.com/news/world-europe-35569094> accessed 12 September 2019

‘Russia’s Approves Information Society Development Strategy through 2030’ (*Meduza*, 10 May 2017) <https://meduza.io/en/news/2017/05/10/russia-s-approves-new-information-society-development-strategy-through-2030> accessed 5 July 2019

Sakenova A, ‘Kleveta v Internete [Internet Slander: Almaly Court Examined the First Case of Insult on the Internet]’ (*Nomad*, 30 January 2013) <http://nomad.su/?a=13-201301300007> accessed 19 June 2019

Salapaeva U, ‘Smozhet Li Marat Asipov Zanimat’sya Zhurnalistikoy? [Will Marat Asipov Be Able to Work as a Journalist?]’ (*Forbes.kz*, 14 August 2019) <https://forbes.kz//process/probing/smojet_li_marat_asipov_zanimatsya_jurnalistkoy_deyatelnostyu/> accessed 16 September 2019

Savitsky V, ‘Kvartal’nyy podschet [Quarterly count]’ (*Comnews*, 2016) <http://www.comnews.ru/content/103556/2016-09-01/kvartalnyy-podschet> accessed 20 September 2019

‘Senatory zapretili popolnyat’ anonimnyye elektronnyye koshel’ki cherez terminaly [Senators banned replenishing anonymous electronic wallets via terminals]’ (*Novayagazeta.ru*, 29 July 2019) <https://www.novayagazeta.ru/news/2019/07/29/153746-senatory-zapretili-popolnyat-anonimnye-elektronnye-koshelki-cherez-terminaly> accessed 2 August 2019

‘Servis Tumblr Zablokirovali v Kazakhstane Iz-Za Propagandy Terrorizma i Pornografii [Tumblr Service Blocked in Kazakhstan Due to Propaganda of Terrorism and Pornography]’ (*Tengrinews.kz*, 11 April 2016) <https://tengrinews.kz/internet/servis-Tumblr-zablokirovali-kazahstane-iz-za-propagandyi-292453/> accessed 22 June 2019

Shanghai Cooperation Organization (SCO), ‘Shanghai Convention on Combating Terrorism Separatism and Extremism’ (15 June 2001) <https://www.un-ilibrary.org/peacekeeping-and-security/international-instruments-related-to-the-prevention-and-suppression-of-international-terrorism_d6956b09-en> accessed 16 August 2019

Shynkarenko O, ‘Zashmorh Na Internet [A Noose on the Internet]’ (8 January 2014)

<http://www.theinsider.ua/business/52bac42dd8f4d/> accessed 7 July 2019

Sikorskaya I, 'V Kyrgyzstane smeshany ponyatiya razzhiganiya rozni i ekstremizma. K chemu eto privodit? [The concepts of inciting hatred and extremism are mixed in Kyrgyzstan. What does this lead to?]' (*Kaktus.media*, 8 October 2018) <https://kaktus.media/doc/379652_v_kyrgyzstane_smeshany_poniatiia_razjiganiia_rozni_i_ekstremizma._k_chemy_eto_privodit.html> accessed 14 September 2019

Simms D and Ghernaouti S, 'Report on Taxonomy and Evaluation of Existing Inventories' (European Union E-Crime Project 2014) <www.ecrime-project.eu/wp-content/uploads/2015/02/E-Crime-Deliverable-2-1-20141128_FINAL.pdf> accessed 8 December 2017

Sindelar D, 'The Kremlin's Troll Army' (*The Atlantic*, 12 August 2014) <https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/> accessed 12 September 2019

'Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' (The American Association for the International Commission of Jurists 1985) <https://www.icj.org/siracusa-principles-on-the-limitation-and-derogation-provisions-in-the-international-covenant-on-civil-and-political-rights/>

Siruk M, 'Ukrayina maye otrymaty chitku perspektyvu chlenstva v ES [Ukraine should get a clear prospect of EU membership - Timothy Garton Ash]' (*The Day*, 11 June 2019) <https://day.kyiv.ua/uk/article/svitovi-dyskusiyi/ukrayina-maye-otrymaty-chitku-perspektyvu-chlenstva-v-yes> accessed 25 June 2019

Smayil M, 'Zapretit' anonimnyye onlayn-platezhi namereny v Kazakhstane [Kazakhstan plans to prohibit anonymous online payments]' (*Tengrinews.kz*, 26 September 2018)

<https://tengrinews.kz/kazakhstan_news/zapretit-anonimnyie-onlayn-plateji-namerenyi-v-kazahstane-354366/> accessed 2 August 2019

Soldatov A and Borodan I, 'Russia's Surveillance State' (12 September 2013) <https://worldpolicy.org/2013/09/12/russias-surveillance-state/> accessed 5 July 2019

Soldatov A and Borogan I, 'In Ex-Soviet States, Russian Spy Tech Still Watches You' [2012] *Wired* <https://www.wired.com/2012/12/russias-hand/> accessed 18 August 2019

Soldatov O, 'The Russian VPN ban: another round in the battle for a free Internet' (*European Centre for Press and Media Freedom*, 20 September 2017) <https://www.rcmediafreedom.eu/Tools/Legal-Resources/The-Russian-VPN-ban-another-round-in-the-battle-for-a-free-Internet> accessed 16 July 2019

——, 'Is the Ukrainian ban on Russian social media justified?' (*European Centre for Press and Media Freedom*, 1 August 2018) <http://www.rcmediafreedom.eu/Tools/Legal-Resources/Is-the-Ukrainian-ban-on-Russian-social-media-justified> accessed 21 June 2019

Soll J, 'The Long and Brutal History of Fake News' (*POLITICO Magazine*, 18 December 2016) <http://politi.co/2FaV5W9> accessed 17 June 2019

'Soobshcheniye press-sluzhby Prezidenta [Statement from Presiden's Press Office]' (9 May 2017) <https://azertag.az/ru/xeber/Soobshchenie_press_sluzhby_Prezidenta-1090744> accessed 21 July 2019

'SORM-3 Budet Vnedren Do 31 Marta 2015 Goda [SORM-3 Shall Be Implemented by March 31, 2015]' (*Roskomsvoboda*, 11 October 2014) <https://roskomsvoboda.org/8827/> accessed 5 July 2019

'South Ossetia: The Burden of Recognition' (*International Crisis Group,* 2010) 205

https://www.crisisgroup.org/europe-central-asia/caucasus/south-ossetia-burden-recognition accessed 10 February 2019

Spano R, *The Internet and the ECHR - A Paradigm Shift?* (2016) <http://tv.coe.int/ECHR/video.php?v=ECHR_20160118_Spano> accessed 5 February 2018

Stankey R, Frappier D and Guyton BW, 'Prepaid Registration: Will US Consumers Be Required to Show Photo ID When Buying a Cell Phone?' (*Lexology*) <https://www.lexology.com/library/detail.aspx?g=16683847-6b51-4954-8a01-a2d91a3c2bde> accessed 26 June 2019

Startseva T, 'Shchodo Vidpovidal′nosti Vlasnyka Veb-Sayta [On the Responsibility of Website Owners]' (*Liga*, 13 October 2013) <https://blog.liga.net/user/tstartseva/article/12481> accessed 3 September 2019

'Statistika Narusheniy Prava Na Svobodu Vyrazheniya v Kazakhstane Yanvar'-Dekabr' 2017 Goda [Statistics of Violations of the Right to Freedom of Expression in Kazakhstan January-December 2017]' (21 January 2018) <http://www.adilsoz.kz/politcor/show/id/223> accessed 21 July 2019

Sternstein A, 'US Intelligence Community Keys in on the Russian "Troll Army" Manipulating Social Media' (*Nextgov.com*, 17 August 2015) <https://www.nextgov.com/cio-briefing/2015/08/us-intelligence-community-keys-russian-troll-army-manipulating-social-media/119158/> accessed 12 September 2019

'Sud podtverdil zakonnost' blokirovki ZHZH [Court confirmed legitimacy of LiveJournal's block]' (*Zakon.kz*, 18 April 2012) <https://www.zakon.kz/4485779-sud-podtverdil-zakonnost-blokirovki-zhzh.html> accessed 21 July 2019

Suharevskaya A, 'Eksperty otsenili kolichestvo serykh sim-kart v Rossii [Experts estimated

illegal SIMs in Russia]' (*Vedomosti*, 5 July 2019) <https://www.vedomosti.ru/technology/articles/2019/07/05/805917-eksperti-otsenili> accessed 30 July 2019

'Telefonnyye razgovory kazakhstantsev budut zapisyvat' i khranit' [Kazakhstani telephone conversations will be recorded and stored]' (*NUR.KZ*, 19 May 2017) <https://www.nur.kz/1498984-telefonnye-razgovory-kazakhstancev-b.html?> accessed 20 September 2019

'The Azerbaijani Laundromat' (*Organized Crime and Corruption Reporting Project (OCCRP)*, 4 September 2017) <https://www.occrp.org/en/azerbaijanilaundromat/> accessed 22 June 2019

'The Decree of the President of the Republic of Belarus No. 60 "On the Issues to Improve Making Use of the National Segment of Internet" (Unofficial Translation)' (*E-Belarus.ORG*) <http://www.e-belarus.org/docs/decree60.html> accessed 2 July 2019

'The government has banned registration in instant messengers by other people's numbers' (*Habr*, 6 November 2018) <https://habr.com/ru/news/t/428874/> accessed 1 August 2019

'The list of restricted access' (*Belarusian State Telecommunications Inspectorate*) <https://belgie.by/ru/lists_access> accessed 21 June 2019

'The Many Identifiers in Our Pockets: A Primer on Mobile Privacy and Security' (*The Citizen Lab*, 21 May 2015) <https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/> accessed 31 July 2019

'The Results of Tender Purchase No. 2015-280164-P' <http://www.icetrade.by/results/all/view/152319> accessed 24 July 2019

Tiwari A, ‘Everything About Tor: What Is Tor? How Tor Works ?’ (*Fossbytes*, 22 May 2017) <https://fossbytes.com/everything-tor-tor-tor-works/> accessed 19 August 2019

Toguzbayev K, ‘Prezidenty s vozmozhnostyami pozhiznennogo pravleniya [Presidents with life-long rule opportunities]’ (*Radio Free Europe/Radio Liberty Azerbaijani Service*, 12 April 2018) <https://rus.azattyq.org/a/pozhiznennye-praviteli-postsovetskoye-prostranstvo/29160961.html> accessed 26 June 2019

Toleukhanova A, ‘Kazakhstan: Parliament Rams Through Vague Constitution Fix’ (*Eurasianet*, 6 March 2017) <https://eurasianet.org/kazakhstan-parliament-rams-through-vague-constitution-fix> accessed 14 September 2019

——, ‘Kazakhstan: Registration Law Causes Chaos, Forces Apology’ (*Eurasianet*) <https://eurasianet.org/kazakhstan-registration-law-causes-chaos-forces-apology> accessed 21 July 2019

‘Tor FAQ’ (*Tor Project*) <https://2019.www.torproject.org/docs/faq> accessed 3 August 2019

TorGuard, ‘Why TorGuard Has Removed All Russian Servers’ (2018) <https://torguard.net/blog/why-torguard-has-removed-all-russian-servers/> accessed 24 June 2019

Traynor I, ‘EU Pact Challenges Russian Influence in the East’ *The Guardian* (7 May 2009) <https://www.theguardian.com/world/2009/may/07/russia-eu-europe-partnership-deal> accessed 9 August 2019

Trenin D, ‘Welcome to Cold War II’ (*Foreign Policy*, 4 March 2014) <https://foreignpolicy.com/2014/03/04/welcome-to-cold-war-ii/> accessed 12 September 2019

Tselikov A, 'Lurkmore or Lurkless? The Russian Internet Blacklist In Action' (*Global Voices*, 14 November 2012) <https://globalvoices.org/2012/11/14/lurkmore-or-lurkless-the-russian-internet-blacklist-in-action/> accessed 21 July 2019

'Ukraine Blocks Russian Social Networks and Expands Economic Sanctions Against Russian Companies' (*Platform to promote the protection of journalism and safety of journalists*, 17 July 2017) <https://rm.coe.int/ukraine-en-reply-ukraine-blocks-russian-social-networks-and-expands-ec/168073254f> accessed 16 July 2019

'Ukraine President Signs Constitutional Amendment On NATO, EU Membership' (*RadioFreeEurope/RadioLiberty*) <https://www.rferl.org/a/ukraine-president-signs-constitutional-amendment-on-nato-eu-membership/29779430.html> accessed 11 March 2020

Ungku F, 'Factbox: "Fake News" Laws around the World' *Reuters* (2 April 2019) <https://www.reuters.com/article/us-singapore-politics-fakenews-factbox-idUSKCN1RE0XN> accessed 20 June 2019

Usenova B, 'V KR po stat'ye 299 cheloveka mogut posadit' za vpolne bezobidnyye frazy [In the Kyrgyz Republic, under Article 299, people can be imprisoned for uttering completely harmless phrases]' (*Radio Azattyk*, 3 May 2018) <https://rus.azattyk.org/a/kyrguzstan-usenova-law/29206193.html> accessed 14 September 2019

'Uzbek Strongman's Death Confirmed' (2 September 2016) <https://www.bbc.com/news/world-asia-37260375> accessed 25 June 2019

'V Kazakhstane Stali Massovo Blokirovat' Sayty [Kazakhstan Began Mass Blockings of Web Sites]' (*Roskomsvoboda*, 22 October 2015) <https://roskomsvoboda.org/13281/> accessed 21 July 2019

'V Kazakhstane Zablokirovali Sayt s Petitsiyey Protiv Vremennoy Registratsii [Kazakhstan

Blocked Website with Petition against Temporary Registration]' (*Tengrinews.kz*, 9 January 2017) <https://tengrinews.kz/kazakhstan_news/kazahstane-zablokirovali-sayt-petitsiey-protiv-vremennoy-309646/> accessed 22 June 2019

'V Rossii nachali blokirovat' Zello. Chto eto i kto ot etogo postradayet? [Russia began to block Zello. What is it and who will suffer? Q&A on the app used by the protesting truckers]' (*Meduza*) <https://meduza.io/feature/2017/04/14/v-rossii-nachali-blokirovat-zello-chto-eto-i-kto-ot-etogo-postradaet> accessed 27 June 2019

Vergun D, 'V Ukraine Zablokiruyut Yeshche 180 Saytov – SBU Nastaivayet [180 More Sites Will Be Blocked in Ukraine - SBU Insists]' (*UBR*, 13 July 2018) <https://ubr.ua/market/telecom/v-ukraine-zablokirujut-eshche-180-sajtov-sbu-nastaivaet-3873006> accessed 21 June 2019

Verkhovsky A, 'A New Turn of the Kremlin's Anti-Extremist Policy' (*SOVA Center*, 2019) <http://www.sova-center.ru/en/misuse/reports-analyses/2019/04/d40960> accessed 14 September 2019

Versteeg M, 'What Europe Can Teach America About Free Speech' (*The Atlantic*, 19 August 2017) <https://www.theatlantic.com/politics/archive/2017/08/what-europe-can-teach-america-about-free-speech/537186/> accessed 14 August 2019

'Vimeo.com zablokirovan v Kazakhstane [Vimeo.com is blocked in Kazakhstan]' (*Tengrinews.kz*, 22 September 2015) <https://tengrinews.kz/kazakhstan_news/Vimeocom-zablokirovan-v-kazahstane-281282/> accessed 22 June 2019

Vitvitsky B, 'Why Is Raising the Level of Rule of Law In Post-Soviet Ukraine Such a Challenge?' (*VoxUkraine*, 16 September 2019) <https://voxukraine.org/en/why-is-raising-the-level-of-rule-of-law-in-post-soviet-ukraine-such-a-challenge/> accessed 8 March 2020

‘Vizhu novosti, chto na izolyatsiyu interneta potratyat iz byudzheta to li pochti dva, to li 20 milliardov rubley. Tak skol’ko? (Spoyler: neizvestno) [I see the news that almost two, or 20 billion rubles will be spent on isolating the Internet from the budget. So, how much? (Spoiler: unknown)]’ (*Meduza*, 7 February 2019) <https://meduza.io/feature/2019/02/07/vizhu-novosti-chto-na-izolyatsiyu-interneta-potratyat-iz-byudzheta-to-li-pochti-dva-to-li-20-milliardov-rubley-tak-skolko-spoyler-neizvestno> accessed 5 July 2019

‘Vo Vtorom Chtenii Prinyaty Popravki v Zakon o Protivodeystvii Ekstremistskoy Deyatel’nosti [The Second Reading Adopted Amendments to the Law on Countering Extremist Activities]’ (*For.kg*, 2013) <https://www.for.kg/news-216159-ru.html> accessed 14 September 2019

Volz D and Cullison A, ‘“Putin Has Won”: Mueller Report Details the Ways Russia Interfered in the 2016 Election’ *Wall Street Journal* (19 April 2019) <https://www.wsj.com/articles/putin-has-won-mueller-report-details-the-ways-russia-interfered-in-the-2016-election-11555666201> accessed 18 August 2019

Walt SM, ‘History Shows Caution Is the Best Approach for Foreign Action’ (*The New York Times*, May 2015) <https://www.nytimes.com/roomfordebate/2014/09/02/is-dont-do-stupid-stuff-the-best-foreign-policy-30/history-shows-caution-is-the-best-approach-for-foreign-action> accessed 11 March 2020

Washburn D, ‘Religious Tradition and Innovation in the Post-Soviet World: A Case of Revival of Rejection’ (Cumberland Lodge 2007) <https://www.cumberlandlodge.ac.uk/sites/default/files/public/Religious%20Tradition%20and%20Innovation%20in%20a%20Post%20Soviet%20World.pdf> accessed 14 September 2019

‘“We Live in Constant Fear”: Possession of Extremist Material in Kyrgyzstan’ (*Human Rights Watch*, 17 September 2018) <https://www.hrw.org/report/2018/09/17/we-live-constant-fear/possession-extremist-material-kyrgyzstan> accessed 25 June 2019

Webb I, ‘Russia Blocks Walkie-Talkie App Zello As Truckers Strike’ (*Global Voices*, 10 April 2017) <https://globalvoices.org/2017/04/10/russia-blocks-walkie-talkie-app-zello-as-truckers-strike/> accessed 27 June 2019

Webster R, ‘Kazakhstan: Localization of Personal Data’ (*DAC Beachcroft*, 1 January 2016) <https://www.dacbeachcroft.com/en/gb/articles/2016/january/kazakhstan-localization-of-personal-data> accessed 4 July 2019

‘“We Will Find You, Anywhere": The Global Shadow of Uzbekistani Surveillance’ (Amnesty International 2017) EUR 62/5974/2017 <https://www.amnesty.org/download/Documents/EUR6259742017ENGLISH.PDF>

‘What Is a Proxy Service? - Definition from Techopedia’ (*Techopedia.com*) <https://www.techopedia.com/definition/31705/proxy-service> accessed 19 August 2019

‘What Is a URL? - Definition from Techopedia’ (*Techopedia.com*) <https://www.techopedia.com/definition/1352/uniform-resource-locator-url> accessed 8 October 2019

‘What Is an IP Address? - Definition from Techopedia’ (*Techopedia.com*) <https://www.techopedia.com/definition/2435/internet-protocol-address-ip-address> accessed 19 August 2019

‘What Is Anonymizer? - Definition from Techopedia’ (*Techopedia.com*) <https://www.techopedia.com/definition/23133/anonymizer> accessed 18 August 2019

‘What Is Deep Packet Inspection?’ (*CactusVPN*) <https://www.cactusvpn.com/beginners-guide-to-online-privacy/what-is-deep-packet-inspection/> accessed 19 August 2019

‘What Is IP Address Blocking? - Definition from Techopedia’ (*Techopedia.com*) <https://www.techopedia.com/definition/3991/ip-address-blocking> accessed 19 August 2019

‘What Is Violent Extremism?’ (*Federal Bureau of Investigation*) <https://www.fbi.gov/cve508/teen-website/what-is-violent-extremism> accessed 10 August 2019

Whitfield T, ‘The Basque Conflict and ETA’ (United States Institute of Peace 2015) <https://www.usip.org/sites/default/files/SR384-The-Basque-Conflict-and-ETA-The-Difficulties-of-An-Ending.pdf> accessed 13 August 2019

‘Wikimedia Foundation Governance Wiki’ <https://foundation.wikimedia.org/wiki/Home> accessed 21 July 2019

‘Yanukovych Commits Ukraine to Authoritarian Path’ (*RSF*, 20 January 2014) <https://rsf.org/en/news/yanukovych-commits-ukraine-authoritarian-path> accessed 23 June 2019

‘Yet Another Intimidatory Signal to Independent News Media’ (*RSF*, 10 February 2015) <https://rsf.org/en/news/yet-another-intimidatory-signal-independent-news-media> accessed 23 June 2019

‘Zakonoproyekty Ozerova i Yarovoy Ne Snizyat Terroristicheskoy i Ekstremistskoy Ugrozy i Nuzhdayutsya v Pererabotke [Bills by Ozerov and Yarovaya Will Not Reduce the Terrorist and Extremist Threats and Need to Be Improved]’ (*Council under the President of the Russian Federation on the development of civil society and human rights*, 2016)

<http://president-sovet.ru/presscenter/news/read/3151/> accessed 20 September 2019

Zakusylo M, 'Deputaty khochut′ uzakonyty dosudove blokuvannya internet-resursiv [MPs want to legalize extra-judicial blocking of internet resources]' (*detector.media*, 12 July 2017) <https://detector.media/infospace/article/127856/2017-07-12-deputati-khochut-uzakoniti-dosudove-blokuvannya-internet-resursiv/> accessed 22 June 2019

'Zarubezhnym sotssetyam vydvinut trebovaniya po razmeshcheniyu serverov v RK [Foreign social networks put forward requirements for the placement of servers in the Republic of Kazakhstan]' (*Profit.kz*, 2 November 2017) <https://profit.kz/news/42724/Zarubezhnim-socsetyam-vidvinut-trebovaniya-po-razmescheniu-serverov-v-RK/> accessed 4 July 2019

'Zashchitit Li Konstitutsiya Kyrgyzskoy Respubliki Veruyushchikh Ot Ugolovnogo Presledovaniya Za Deystviya, Ne Predstavlyayushchiye Obshchestvennoy Opasnosti [Will the Constitution of the Kyrgyz Republic Protect Believers from Criminal Prosecution for Actions That Do Not Pose a Public Danger?]' (*Koom.kg*, 2017) <http://www.koom.kg/index.php?act=material&id=3762> accessed 14 September 2019

Zee B van der, 'How Reader Funding Is Helping Save Independent Media across the World' *The Guardian* (25 December 2017) <https://www.theguardian.com/technology/2017/dec/25/how-reader-funding-is-helping-save-independent-media-across-the-world> accessed 2 August 2019

'Zheleznyak: Prodazha SIM-Kart v Rossii Nosit Nesistemnyy Kharakter [Zheleznyak: Saling of SIM-Cards in Russia Is Non-Systemic]' (*Edinaya Rossiya*, 22 October 2013) <http://www.er-duma.ru/press/61185/> accessed 30 July 2019

Zhulmukhametova Z, 'Privyazyvat' Nomera Telefonov Abonentov k IIN Nachnut Uzhe Letom 2018 Goda [Binding the Phone Numbers of Subscribers to the Identification Numbers

Will Begin in the Summer of 2018]' (16 May 2018) <https://informburo.kz/novosti/privyazyvat-nomera-telefonov-abonentov-k-iin-nachnut-uzhe-letom-2018-goda.html> accessed 27 June 2019