PRIVACY, ENCRYPTION AND HUMAN RIGHTS: A COMPARATIVE ANALYSIS OF ANTI-ENCRYPTION POLICIES IN RUSSIA AND TURKEY AND THEIR EFFECT ON HUMAN RIGHTS ACTORS

By Anastasia Vladimirova

MA Human Rights. Long Thesis
Professor: Dr. Sejal Parmar
Legal Studies Department
1051 Budapest, Nador utca 9
Hungary

Table of Contents

Abstract

This essay aims to develop a critical approach to encryption and its role in ensuring the exercise of human rights in the digital age, specifically the right to privacy and the right to free expression. In light of increasing attempts by states to restrict the use of cryptographic technologies,[1] the author will focus on two unique case-studies – Russia and Turkey. In Turkey, following the attempted coup in July 2016, the authorities used the state of emergency to target activists, journalists and human rights defenders, specifically within the context of using encrypted communication tools.[2] In Russia, several controversial amendments to the existing counter-terrorism laws were passed over the recent years that directly target encryption communication.[3] As such, the two countries represent distinct examples of how governments rely on domestic anti-terrorism legislation and invoke national security to constrict online spaces, particularly the use of encryption technologies.

Starting with setting out conceptional and theoretical frameworks for privacy and freedom of expression, the author will analyze scholarly works that shaped both concepts. The author will further focus on the comparative analysis of the laws that govern the use of encryption in Turkey and Russia, arguing that by invoking the notions of national security, non-democratic states bypass their obligations under international human rights law in order to restrict the use of encryption among human rights actors and members of the civil society. The author will then discuss the common themes emerging from evaluation

[1] 'The international encryption debate: privacy versus big brother' (LEXOLOGY, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 3 September 2019

[2] 'Encryption At The Centre Of Mass Arrests: One Year On From Turkey's Failed Coup' (Privacy International, 18 July 2017) <https://medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9> accessed 6 September 2019

[3] '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 17 October 2018

of the situations in Russia and Turkey and will make several concrete recommendations which could help address challenges posed to the use of encryption by non-democratic states. Finally, based on the argument that encryption is intimately interconnected with the rights to privacy and freedom of expression, as evident from the two case-studies, the author will argue that due to its enabling and protective function, encryption requires special protection under international human rights law.

Introduction

Real world problem in context

Communication is an essential aspect of interactions and relationships between individuals. Communication between people enables expression, exchange and learning of information. It can be argued that communication is the most important aspect of human rights work conducted by human rights defenders, advocates, civil society organizations and journalists, making information exchange and communication between these actors highly important and particularly sensitive in hostile contexts.[4]

With the advancement of the Internet and modern technologies, the nature of threats that human rights actors experience as a result of interference with their communication and information flows has not changed; rather, these threats represent expanded and extended versions of already existing forms to control and constrict activists' freedom of expression, association and assembly.[5]

4 Hankey, Stephanie & O Clunaigh, Daniel. *Rethinking Risk and Security of Human Rights Defenders in the Digital Age*. Journal of Human Rights Practice, Vol. 5, November 2013, p. 537

5 Ibid

As threats to human rights advocates' communication and information-sharing developed, so did the security and protection tools. Today, technologies that aim to protect individuals' rights in the digital sphere have become increasingly available and human rights defenders employ many such tools to protect themselves from targeted surveillance, unlawful interference, coercion and threats from their adversaries, such as businesses, authoritarian governments, as well as private and non-state actors. Among such tools are VPNs (Virtual Private Networks), secure encrypted messengers (Telegram, Signal and WhatsApp), email and file encryption tools (PGP).

Encryption has for a long time been a key solution for securing online communications. It is widely used by activists to protect their communications and information, which is crucial for ensuring their own and their colleagues' security, protecting personal, valuable and sensitive data – all of which is essential for effective human rights work. Encryption tools not only provide protection of online correspondence, but also help human rights actors remain anonymous.

Anonymity is another way to protect one's communications and information and, therefore, ensure the safety of those involved in human rights work. By allowing anonymity, encryption tools increase the sense of security and protection from all kinds of unwanted interference, enabling secure communication and, as a result, more freedom to express oneself freely and openly in a private manner.

Jurisdictions

Over recent years, the very tools that human rights activists rely on (VPNs, secure messaging apps, anonymizers) have been targeted by governments through the adoption and/or application of counterterrorism and counterextremism laws and policies. The Freedom on the Net Report 2017 highlights a shared trend among a number of states[6] to introduce new legislation demanding ban or restriction of anonymity tools and providing back doors to encrypted communications of individuals.[7]

In Turkey and Russia, the extent with which the governments have targeted encryption and anonymity has grown over the past several years. Both countries represent distinctive examples of how governments rely on domestic anti-terrorism legislation and invoke national security to constrict online spaces, particularly the use of encryption technologies.

In Turkey, following the attempted coup in July 2016, the authorities used the state of emergency to target activists, journalists and human rights defenders, specifically within the context of using encrypted communication tools.[8] In Russia, a number of controversial amendments to the existing counter-terrorism

[6] Encryption restrictions – China, Hungary, Russia, Thailand, the United Kingdom, and Vietnam; VPN restrictions – Belarus, China, Egypt, Russia, Turkey, and the UAE

[7] Freedom on the Net 2017, Freedom House 2017, p. 20,

[8] 'Encryption At The Centre Of Mass Arrests: One Year On From Turkey's Failed Coup' (Privacy International, 18 July 2017) <https://medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9> accessed 6 September 2019

laws were passed over the recent years that directly target encryption communication.[9] Therefore, the two states present an opportunity for in-depth and challenging comparative analysis.

What are states' justifications for cracking down on encryption and anonymity tools? Why do states employ specific anti-extremist and anti-terrorism rhetoric when coming up with restrictive policies on encryption and anonymity? Does Turkey's rational differ from the one of Russia and vice versa? Or, are these rationales similar despite different political situations in the countries in question? This essay will attempt to answer these and other questions.

Research question

This essay aims to critically evaluate the existing legislation that governs the use of cryptographic technology in Russia and Turkey, as well as look at the effects that such legislation has on human rights actors and ordinary individuals. In particular, the author poses the following questions: in what ways do counterterrorism laws and measures affect, impede and interfere with the work of human rights actors and civil society? What do these trends say about an overarching ideological framework that informs these countries' approach to encryption? What are the relative flaws and strengths of such laws from the international human rights law perspective? How does international human rights law approach the increasingly growing worldwide trend towards banning encryption? Finally, how do these case studies

[9] '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 17 October 2018

reflect the existing encryption debate which often juxtaposes privacy of an individual and security of the state as mutually exclusive ideas?[10]

The author's main argument is that non-democratic governments invoke national security and the necessity of counter-terrorism measures to target the use of encrypted communications by human rights actors and civil society. This is often done with the help of legislative amendments that help to bypass constitutional protections and as such threaten the exercise of human rights, particularly the rights to freedom of expression and privacy. More often than not, such deliberate targeting of security-oriented tools directly affects the work of human rights activists and other civil society actors. This is done in spite of binding obligations that countries like Russia and Turkey have under international human rights law.

Methodology

The author's research methodology is mainly focused on desk research, guided by consultative interviews with human right activists and digital security consultants working in Russia and Turkey. Desk research will be mostly comprised of examining relevant legislation, as well as secondary sources. Additional information and resources may be drawn from the author's consultations with scholars during the Freedom Online Coalition Conference in November 2018, the Internet Freedom Festival in April 2019 and the Dublin Platform for Human Rights Defenders in October 2019. The methodology will also include application of the comparative approach towards the analysis of the two jurisdictions, as well as their analysis from the perspective of international human rights law.

[10] 'The international encryption debate: privacy versus big brother' (LEXOLOGY, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 3 September 2019

Conceptual framework

In this section, the author will look at the key concepts addressed in the essay – privacy and freedom of expression. The author will look at the rationales for both concepts and situate the two in the context of human rights work, specifically as they relate to the work of human rights actors and their digital communications. The author will show why and how privacy and freedom of expression and opinion are interconnected in online communications. Finally, the author will focus on analyzing why secure communication, enabled by encryption, is essential for exercising freedom of expression.

This thesis attempts to analyze legislation targeting encryption in online communications in Turkey and Russia and assesses whether laws pose a threat to the exercise of the right to privacy and the right to freedom of expression in their respective societies.

To set the broader international legal context of the comparative analysis, it is necessary to lay out international standards governing the exercise of the right to privacy and the right to free expression.

Both the right to freedom of expression and the right to privacy are protected by core international legal documents. The Universal Declaration on Human Rights (UDHR), as soft law, sets forth the universal principles that should be applied to free speech and privacy across the globe in the states that have endorsed the document.[11] The International Covenant on Civil and Political Rights (ICCPR), as hard law, is a binding document and obliges all those State who have ratified the treaty to respect the rights embodied in it.

[11] The Universal Declaration on Human Rights (UDHR), Article 12 and Article 19

It is important to assess rights to freedom of expression and privacy in Turkey and Russia from the perspective of the regional legal document which has a binding effect on both states as a result of ratification. As Member States of the European Council[12], Russia and Turkey have ratified the European Convention on Human Rights (ECHR) and are both bound by the standards set in the document. In ECHR, the right to privacy is formulated in Article 8, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence."[13]

The phrasing of the freedom of expression and privacy standards in both soft and hard law is almost identical and reflects the same set of values. Freedom of expression encompasses the unrestricted right to search for, access and interpret information through any means.

Encryption enables an individual to exercise both rights, particularly the key aspects identified in the core international documents - the right to search for and access information, to hold an opinion and the respect and inviolability of private correspondence. Encryption also protects both freedom of expression and privacy from the "interference of public authority." As such, encryption carries an enabling and a protecting function when it comes to exercise of freedom of expression and opinion and privacy. These enabling and protective functions are especially important for realization of these rights in states where freedom of expression is limited and where privacy is subject to interference.

[12] Turkey became COE's Member State on 13 April 1950, Russia became its Member State on 28 February 1996 https://www.coe.int/en/web/portal/47-members-states

[13] The European Convention on Human Rights (ECHR), Article 8

Freedom of Expression

Article 19 of the UDHR states that "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."[14] Article 19 of ICCPR states:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.[15]

Article 10 of ECHR states, "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…".[16]

[14] UDHR, Article 19
[15] International Covenant on Civil and Political Rights (ICCPR), Article 19
[16] ECHR, Article 10

It is crucial to note that the limitations provided to article 19(3) are only applicable to article 19(2), the right to freedom of expression, but not to article 19(1), the right to hold opinions without interference.[17]

There are several works of scholars who articulated rationales for freedom of expression that are crucial to mention in this essay. Scholar Eric Barendt puts forward four distinct arguments commonly used to justify the free speech principle. The first argument suggests that freedom of expression as a facilitator of open discussion is necessary for discovering truth.[18] Secondly, free speech plays role in one's self-fulfillment and autonomy. Barendt points out that free speech is linked directly to other fundamental rights, such as freedom of religion, thought and consciousness.[19] Its restrictions can impede the growth of one's personality.[20]

The third argument puts free speech as an essential aspect of one's participation in a democracy. Barendt writes that a truly democratic society is possible only when citizens have access to the discovery and spread of truth, by means of which they are able to make informed decisions.[21] The fourth and final argument focused on "the evils of regulation, rather than the good of free speech."[22] The author specifically points out that governments and other authorities can outlaw accurate speech and suppress ideas the influence of which they have reasons to fear.[23] The laws can also be applied to cover the expression of radical and subversive ideas.[24]

17 United Nations, Human Rights Committee, General Comment No. 34, CCPR/C/GC/34
18 Barendt, E. M. *Freedom of Speech.* Oxford University Press, 2007 p. 8
19 Ibid p.13
20 Ibid
21 Ibid p.18
22 Ibid p. 21
23 Ibid
24 Ibid

Another way to look at the freedom of speech is to assess it from the perspective of interest of the speaker, the audience and the bystander. Barendt suggests that "speakers and other communicators generally have a close, perhaps an intense, involvement with the content of their message, whether it is political, literary or artistic."[25] This and above mentioned perspectives are highly relevant to the work of the human rights actors, as the content of their communications has a very important, urgent character. They can be intensely and closely involved with the content of their communications as regards personal or sensitive information about their work, projects, whereabouts, as well as the same information concerning more people, involved in the cause.

However, the perspective of the speaker carries just a partial significance for the justification of the free speech principle. Some of the rationales reflect the importance that speech carries for the audience. As such the content of the message might be of utmost value to an individual from the perspective of self-realization and autonomy of the individual; it can also be of crucial importance to the audience when it comes to the pursuit of truth and ensuring democracy.

However, the speaker and the audience are never the only parties engaged in the exercise of free expression. Governments, as the primary guarantors of their citizens' rights, define the extent to which the rationales behind the free speech principle inform the exercise of the right. The position of the government and its influence on the exercise of the free speech has occupied the central place in the freedom of expression debates.[26] It is so because the government, by its nature, is a controlling body and

[25] Ibid pp. 23-24
[26] Sajo, Andras. *Freedom of Expression.* Institute of Public Affairs, 2004, pp. 15-16

freedom of expression can be regarded as a measure of the level of government's control over its citizens. Professor Andras Sajo noted, "The very nature of government, considering the impact on society, requires the utmost (self-)restriction in the part of the state in regulating speech, as all restrictive measures will further increase the towering presence of governmental views."[27] Sajo compares freedom of speech to imposing restrictions on the state and argues that it "is necessary for the functioning of a liberty-preserving democracy."[28] Sajo's argument suggests that state's ideology has direct connection to the level of freedom of expression in a society.

Despite the fact that the arguments for freedom of expression and its rationales have been shaped and solidified over centuries of scholarly debate, the exceptions set out in international human rights law, such as ICCPR and ECHR, can be applied to the rights resulting in restrictions of freedom of expression. Both ICCPR and ECHR allow for such restrictions in the name of national security public order and morals.[29]

Privacy

Article 12 of the UDHR states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence…".[30] Similarly, word to word, the ICCPR states in Article 17(1) that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence…".[31] Article 8 of the ECHR also focuses on one's privacy, family, home and

[27] Ibid, p. 19
[28] Ibid
[29] ICCPR, Article 19 (3); ECHR, Article 10 (2)
[30] UDHR, Article 12
[31] ICCPR, Article 17(1)

correspondence, stating: "Everyone has the right to respect for his private and family life, his home and his correspondence."[32]

Scholars have for a very long time tried to define privacy. One of the most commonly referenced pieces of scholarly work dedicated to formulating the right to privacy was written in 1890 by Samuel D. Warren and Louise D. Brandeis, two legal scholars at Harvard University.[33] The article titled "The Right to Privacy," has been referred to by many scholars in an attempt to determine the roots of the concept in the contemporary legal and academic fields. Professor of Law Dorothy J. Glancy wrote in her article titled "The Invention of the Right to Privacy," that Warren and Brandeis "invented a legal theory which brought into focus a common 'right to privacy' denominator already present in a wide variety of legal concepts and precedents from many different areas of the common law."[34] In her article, Glancy highlights what she considers the key phrasing in Warren and Brandeis' work that gives definition to the right to privacy: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others … fix[ing] the limits of the publicity which shall be given them."[35] She suggests that to its inventors, "the right to privacy meant that each individual had the right to choose to share or not to share with others information about his or her 'private life, habits, acts, and relations.'"[36]

[32] ECHR Article 8
[33] Warren D., Samuel & Brandeis D. Louis. *The Right to Privacy.* Harvard Law Review, Vol. 4, No 5, December 15, 1890, pp. 193-220

[34] Glancy J., Dorothy. *The Invention of the Right to Privacy.* Arizona Law Review, Vol. 21, 1979, p. 3
[35] Ibid, p. 2
[36] Ibid, p. 3

In tracing the drafting history of the right to privacy, scholars Oliver Diggelmann and Maria Nicole Cleis discovered that long before the right to privacy was articulated in constitutions, it was recognized internationally, such as in the Universal Declaration of Human Rights.[37] Moreover, only some aspects of privacy have been articulated by the drafters, which most commonly included inviolability of home, correspondence, family life, as well as protections from unreasonable searches of the body.[38]

It can be argued that it is precisely because privacy as a concept covers so many aspects and extends to different spheres of life, that the attempts to come up with one precise definition for it still continue today. With the introduction of technology into almost every aspect of our lives, the common and traditional definitions of privacy have been challenged while the legal concept required rethinking and reflection on par with technological progress.

This perspective finds support in the vision of privacy expressed by a computer science scholar James H. Moor, who has argued that privacy is "a matter of individual preference, culturally relative, and difficult to justify in general."[39] Moor's conceptualization of privacy represents a technologist's point of view, and at the same time points at the same problem which has been highlighted by many legal scholars – the difficulty in finding a strict definition of privacy.

[37] Diggelmann, Oliver & Cleis, Maria Nicole. *How the Right to Privacy Became a Human Right.* Human Rights Law Review, Vol. 14, 2014, p. 441
[38] Ibid pp. 441- 442
[39] Moor H, James. *Towards a Theory of Privacy in the Information Age.* Computer and Society, September 1997, p. 28

The United Nations Special Rapporteur on the right to privacy, Joe Canatacci, has argued that "privacy is a dynamic right, not a static right"[40] and that the understanding and the exercise of the right to privacy have "varied across the dimensions of 'Time, Place and Space.'"[41] He argues:

> Instead, it makes one reflect about the complex set of values that underpin the right and the way that our understanding of the right needs to change as circumstances change in order for the underlying values to continue to be protected and indeed, as much as possible, have their protection increased.[42]

With the advent of technology, the concept of privacy has expanded in scope and therefore in definition. The invention of the Internet and the subsequent rapid development of technologies have resulted in new dimensions of privacy, which needed to be identified, defined and balanced with existing privacy regulations.

It has been reiterated that the right to privacy is instrumental to the exercise of other human rights both online and offline.[43] The close connection between the right to privacy and the right to free expression has been recently explored by scholar Sandra Wachter in her essay titled "Privacy: Primus Inter Pares. Privacy

[40] United Nations, General Assembly, *Report of the Special Rapporteur on the Right to Privacy, A/HRC/ 34/60*, para 22
[41] Ibid
[42] Ibid
[43] United Nations, Human Rights Council, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/39/29 para. 11; United Nations, Human Rights Committee, General Comment No. 34, CCPR/C/GC/34 para. 1

as a Precondition for Self-Development, Personal Fulfillment and the Free Enjoyment of Fundamental Human Rights."

In her essay, Wachter articulated her understanding of privacy based on the analysis of a number of landmark cases from the European Court of Human Rights (ECtHR). Relying on the jurisprudence of the ECtHR, the author argues that there is "an inherited hierarchy among certain human rights in which privacy occupies an elevated position."[44] She suggests that this is due to the role privacy plays in realization of other human rights embodied in the ECHR, particularly highlighting freedom of expression and freedom of thought.[45]

The author suggests three concepts of privacy – "internal privacy," "external privacy" and "premium privacy."[46] The concept of "internal privacy" rests on three rationales – development and fulfillment of personality, tolerance and equality and informational self-determination.[47]

First, she argues that privacy is an essential precondition for development and fulfillment of one's personality.[48] Privacy provides protection for what the author calls "areas that are closely connected to human nature and essential to build one's character," such as personal and family life, home and personal correspondence.[49] The protections under Article 8 in the interpretation of the Court also extend to other areas of one's life such as, for instance, the free choice and exercise of the occupation and the protection

[44] Wachter, Sandra. *Privacy: Primus Inter Pares. Privacy as a Precondition for Self-Development, Personal Fulfillment and the Free Enjoyment of Fundamental Human Rights.* University of Oxford, October 2016, p.4
[45] Ibid, p. 4
[46] Ibid, pp. 4-5
[47] Ibid, p. 5
[48] Ibid, p. 6
[49] Ibid, p. 6

of "individual and private communication of with business partners, customers, clients and patients."[50] As such, argues Wachter, the protections of Article 8 extend to relationships with other people, even in public."[51]

Second argument made by Wachter is that privacy is crucial for tolerance and equality.[52] By providing protection for new and changing principles and morals, privacy provides everyone with a supportive environment for continuous process of development and self-fulfillment and as such helps to prevent discrimination.[53]

Finally, the author brings up the concept of informational self-determination, introduced by the German Constitutional Court, which entails that "people have to be in control over how their personal information is handled."[54] The justification for such an argument is that privacy helps protect individuals from discrimination which can result from one's projection or expression of views, such as "religious and political beliefs, gender and sexual preferences and life choices".[55]

Wachter argues that in order to protect themselves from discrimination, people need to feel that the choice to share or not share certain information about themselves as well as who to share it with depends entirely on their free choice.[56] This is what the concept of informational self-determination entails. Therefore, the

[50] Ibid, p. 7
[51] Ibid, p. 7
[52] Ibid, p. 8
[53] Ibid, pp. 8-10
[54] Ibid, p. 10
[55] Ibid, pp. 10-11
[56] Ibid, p. 13

tools which can enhance privacy are important as they help avoid discrimination which can endanger pluralism.[57]

It is hard not to draw parallels between Wachter's analysis of the rationales for privacy and the rationales for freedom of expression covered in the previous section. While the right to freedom of expression is crucial for self-realization, privacy ensures one's development and self-fulfillment. As with the right to freedom of expression, the right to privacy is argued to be essential for sustaining a pluralist society and democracy.

However, there are not just parallels between the rationales for the two rights; privacy, as Wachter points out, is placed high in the hierarchy of rights for a reason – it enables the exercise of other rights, one of them being the freedom of expression.[58] When it comes to freedom of expression, Wachter argues that "development of personality is required to express and hold views and … that free expression of these views call for privacy."[59]

In the age of the Internet and algorithms, freedom of expression cannot be looked at separately from privacy. And privacy as a precondition for freedom of expression cannot be realized without strong protections for the right to privacy. Privacy in the digital age does not mean being let alone or having the door of one's house locked. Neither going alone on a trip to a remote location means privacy. Privacy in the digital age is highly reliant, if not completely dependent, on technology that can be built to erode it or

[57] Ibid, pp. 10-11
[58] Ibid, p. 4
[59] Ibid, p. 13

can be built to protect it. As such, no serious conversation about safeguarding privacy can happen without mentioning technology and tools that define our level of privacy.

When discussing the connection between privacy and freedom of expression, Wachter analyses all three different components of the right, encompassed under Article 10 – the right to form and hold an opinion, the right to express an opinion and the freedom to access, search and impart information. Wachter argues:

> Some level of privacy is required to ensure that people feel safe to form and hold their views, especially if they believe in controversial concepts. Having their views involuntary exposed to the outside world makes them vulnerable to discrimination or victims of public humiliation.[60]

She further argues that "being undisturbed and unmonitored whilst gathering information is necessary to freely exercise this human right."[61]

Wachter's analysis suggests that privacy in and of itself is not enough in the age of digital technology. It is important that individuals take steps to actively protect and enhance their privacy in order to protect themselves from being monitored and prevent any disturbance that the exposure of their personal information can bring.

[60] Ibid, p. 14
[61] Ibid, p. 14

The analysis of a wide range of ECtHR cases that the author presents in her paper indicates the critical role that the ECtHR ascribes to privacy, as a precondition for a range of fundamental human rights and as a right in itself.

Furthermore, the author points out that privacy is a key enabler of pluralism and therefore democracy.[62] It is the private environment in which one can pursue self-fulfillment without fear of being discriminated against that supports the pluralism of views and ideas within the society as a key aspect of democracy.[63]

To conclude, the importance of having access to secure and private communication is of ultimate value for human rights actors. First, it is essential for their self-realization, both personal and professional, in their capacity as human rights advocates. Second, as individuals fighting for justice, equality and human rights, the truth for them is one of the main instruments for achieving their goals. Finally, the fight for human rights is a crucial step for maintaining and achieving democracy. As such, all three rationales of freedom of expression come together as interdependent in the context of human rights work. This poses the immediate question of whether and to what extent secure communication is essential for the realization of all the three rationales of freedom of expression in the context of human rights actors' work.

Encryption

Encryption has long been discussed in the context of freedom of expression and privacy. In his 2015 report to the Human Rights Council, the Special Rapporteur on the promotion and protection of the rights to

[62] Ibid, p. 13
[63] Ibid, p. 13

freedom of opinion and expression, David Kaye, framed encryption as a central issue in the context of free expression and privacy. He stated:

> Encryption and anonymity, today's leading vehicles or online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference, and enabling journalists, civil society organizations, members of ethnic or religious groups, those prosecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression. [64]

In this elaborate definition of encryption and anonymity, Kaye highlights the broad spectrum of professions and communities for whom the tools are essential for the realization of their right to free speech. Kaye describes many individuals and groups who work to promote and protect human rights in their communities and countries, a group which is the focus if the current essay. The author's argument that encryption is essential in the work of human rights activists operating in hostile and risky context finds support in Kaye's further definition of encryption:

> Encryption and anonymity, separately or together, … enable private communications and shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments." [65]

[64] United Nations, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression, David Kaye,* A/HRC/29/32 (22 May 2015) para. 1
[65] Ibid, para. 12

As a result of this intimate link between encryption and the rights to freedom of expression and privacy, some scholars have argued for encryption to be considered a human right. David Casacuberta, an Associate Professor of Philosophy of Science at the Autonomous University of Barcelona, Spain, argues that encryption is "a twenty-first century right."[66] For Casacuberta, the right to encryption is directly connected with the privacy of one's communications. He argues that "the right to decide whom I allow to listen to my conversations" is a right "we have in a physical world" and as such it extends to the digital sphere.[67] Casacuberta is also an advocate for recognition of "the right to electronic privacy [as a] part of the declaration of universal rights and democratic institutions."[68] He suggests that cryptography is the only means by which an "ordinary ICT [information and communications technology] user has the power to protect their electronic communications."[69]

Case-studies: Russia and Turkey

Precedent

The debate surrounding encryption has been ongoing for a long time. With the emergence of this technology and its increased use by the public, governments became worried that not every communication was within their reach anymore. In the wake of the disclosures made by Edward

[66] Plasencia, Adolfo & O'Reilly, Tim, 'Encryption as a human right', *Is the Universe a Hologram? Scientists Answer the Most Provocative Questions.* Cambridge: The MIT Press, 2017. p. 225
[67] Ibid, p. 225
[68] Ibid, p. 231
[69] Ibid

Snowden[70], a few companies that pioneered secure email and messaging clients using encryption as a core protective feature had to shut down their services in response to the US government's request to disclose the cryptographic keys that would enable the government to have access to the private communications of these companies' clients.[71]

The landmark case that opened up a larger debate surrounding encryption and public security was the San Bernardino shooting that claimed the lives of 14 people in San Bernardino, US, in December 2015.[72] In the process of the investigation the Federal Bureau of Investigation (FBI) found the iPhone belonging to one of the perpetrators, but could not search it, as the phone was locked.[73] As a result, a federal judge issued an order requesting Apple to assist the FBI in decrypting the phone,[74] invoking the All Writs Act of 1789. From the FBI's standpoint, it was asking for help in solving an incident deemed a "terrorist attack," and, as such, the agency, as well as the government, viewed the case as a matter of national security.[75] From Apple's standpoint, the request, if met, would have compromised the carefully engineered security software that guaranteed privacy and protection from cyber-attacks and cyber criminals to a vast number of Apple's customers globally.[76] Having fully understood the national security implications of the San Bernardino case, Apple deemed the request "an overreach on the side by the U.S. government" and stated it would not compromise the values of security and privacy that were the building block of iPhone's

70 'Edward Snowden: the whistleblower behind the NSA surveillance revelations' (The Guardian, 11 June 2013) <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> accessed 15 November 2019

71 Plasencia, Adolfo & O'Reilly, Tim, 'Encryption as a human right', *Is the Universe a Hologram? Scientists Answer the Most Provocative Questions.* Cambridge: The MIT Press, 2017, p.232

72 'San Bernardino shooting: what we know so far' (BBC, 11 December 2015)< https://www.bbc.com/news/world-us-canada-34993344> accessed 10 October 2019

73 'Apple v. FBI' (Electronic Privacy Information Center) <https://epic.org/amicus/crypto/apple/> accessed 11 October 2019

74 Ibid

75 Ibid

76 Ibid accessed 13 October 2019

security system.[77] In a statement issued on 16 February 2016, Apple's Chief Tim Cook called the request "a dangerous precedent" and shared a concern:

> If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.[78]

Despite privacy being the central issue in the dispute, freedom of expression had a major role to play in Apple's defense. In the Amici Curiae Brief submitted by the Electronic Frontier Foundation (EFF) and 46 technology and cryptography experts and researchers to the Court, the main argument was that by requesting Apple to build a backdoor into iPhone, the U.S. government compels the company's engineers to say something they do not want to say, namely, to write the code they do not want to write out of their concerns for privacy and security of their customers.[79] In such a scenario, the code which was requested from Apple was considered compelled speech that challenged speaker's beliefs and hindered their ability to communicate their intended message.[80] The brief also states that "computer code, including the code that makes Apple's iOS operating system and its security features including encryption, is a form of protected speech under the First Amendment."[81]

[77] 'A Message to Our Customers' (Apple, 16 February 2016)<https://www.apple.com/customer-letter/> accessed 13 October 2019
[78] Ibid
[79] Brief of Amici Curiae, Electronic Frontier Foundation and 46 technologists, researchers, and cryptographers, 22 March 2016
[80] Ibid p. 7
[81] Ibid p. 13

The dispute between Apple and the FBI, which was widely referred to in the press as "Apple V FBI," has stirred a vigorous debate among the policy makers, privacy advocates and the public about individual's privacy and security of the public in the digital age.[82] Most importantly, it focused the world's attention on encryption, on its role in ensuring our privacy and security and on potential threats that its use can cause to public safety.

In refusing to cooperate with the FBI, Apple defended privacy and security, the values it stands for, and that it offers to millions of its users who choose the company's products for these specific reasons. Nevertheless, since the Apple-FBI dispute over the San Bernardino case, national security and public safety have become the go-to arguments for anti-encryption advocates worldwide.[83]

The 2017 Freedom on Net Report raises concerns over increasing anti-encryption policies in a number of states.[84] The Special Rapporteur on the Right to Privacy, Joe Canatacci, has also observed: "an increased tendency for governments to promote more invasive laws for surveillance, which allow for the thinly disguised permanent mass surveillance of citizens."[85]

The Special Rapporteur on the Right to Freedom of Opinion and Expression, Kaye posited two key questions with regards to encryption. The first asked whether "the right to privacy and freedom of opinion

[82] 'The international encryption debate: privacy versus big brother' (LEXOLOGY, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 3 September 2019

[83] Ibid

[84] Freedom on the Net 2017, Freedom House 2017, p. 20

[85] United Nations, General Assembly, *Report of the Special Rapporteur on the right to privacy* A/71/368, para. 28

and expression protect secure online communication, specifically by encryption…?"[86] Second is "to what extent may Governments, in accordance with human rights law, impose restrictions on encryption and anonymity?"[87] In the United States context, for example, the debate between Apple and the FBI showed that, where constitutionally protected rights, such as freedom of expression, are directly implicated, there is a strong argument for the use of encryption to protect those rights.[88] The second question bears more complexity, especially if posed in context of different countries.

Jurisdiction 1 – Russia

This section will analyze the laws that govern encryption in Russia. It will focus on outlining the protections that the Russian Constitution grants to the right to free speech and opinion and privacy. It will then examine the legislation which proposes restrictions on encryption and analyze it from the standpoint of Russia's commitments under ICCPR and ECHR.

The Constitution of the Russian Federation has provisions concerning both the right to freedom of expression and the right to privacy. Article 23 of Chapter 2, titled "Rights and freedoms of Man and Citizen" states:

> 1. Everyone shall have the right to the inviolability of private life, personal and family secrets, the protection of honour and good name.

[86] United Nations, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression, David Kaye*, A/HRC/29/32 (22 May 2015), para. 3
[87] Ibid, para. 3
[88] 'Apple v. FBI' (Electronic Privacy Information Center) <https://epic.org/amicus/crypto/apple/> accessed 11 October 2019

2. Everyone shall have the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages. Limitations of this right shall be allowed only by court decision.[89]

Article 24 (1) of the Russian Constitution states: "The collection, keeping, use and dissemination of information about the private life of a person shall not be allowed without his or her consent."[90] Article 29 states that "everyone shall be guaranteed freedom of ideas and speech."[91]

Finally, Article 7 of the Russian constitution states that "The Russian Federation is a social State whose policy is aimed at creating conditions for a worthy life and a free development of man."[92] Considering that the guarantees in the Russian Constitution reflect "the universally recognized principles and norms of international law,"[93] it follows that privacy is also protected under the Russian Constitution as an integral part of the development of an individual.

The Russian Constitution allows for restrictions on both the second part of the right to privacy and the right to freedom of expression and freedom of ideas in case "of state of emergency in order to ensure the safety of citizens and the protection of the constitutional system."[94]

In Russia, the Federal Law No. 149-FZ of July 27, 2006 on Information, Information Technologies and the Protection of Information governs the use of encryption and cryptographic technology.

[89] The Constitution of the Russian Federation, Article 23
[90] The Constitution of the Russian Federation, Article 24 (1)
[91] The Constitution of the Russian Federation, Article 29
[92] The Constitution of the Russian Federation, Article 7
[93] The Constitution of the Russian Federation, Article 17
[94] The Constitution of the Russian Federation, Article 56

The law introduces a definition for communication service providers calling them "the organizer of dissemination of information."[95] "The organizer of dissemination of information" is defined by the law as "a person pursuing the activity of ensuring the operation of information systems and/or computer software which are intended and/or used to receive, transmit, deliver and/or process electronic messages of users of the Internet."[96]

Overall, the law requires that the providers of electronic communications services operating on the territory of the country obtain license from the authorities.[97] The exception includes operators of state information systems, municipal information systems and communications operators, who already have a license.[98] According to the law, individuals who use electronic communications services for personal and family needs are also exempt from the responsibility to obtain license.[99]

In Russia, the one and only precedent that resulted from this legislation was the blocking of the Russian messaging app Telegram, after its creator Pavel Durov refused to share encryption keys with the Russian Federal Security Services (FSB).[100]

95 Federal Law No. 149-FZ of July 27, 2006 on Information, Information Technologies and the Protection of Information, Article 10.1.1
96 Ibid
97 Ibid, Article 10.1.5
98 Ibid
99 Ibid
100 'Telegram CEO Durov Says Russia's FSB Demands Messenger's Encryption Keys' (RFE/RL, 27 September 2017)<https://www.rferl.org/a/telegram-durov-russia-fsb-encryption-keys-security/28760575.html> accessed 10 November 2019

Since the law was signed in 2006, a number of amendments have been passed, but those that had a visible effect on encryption and private communications have been introduced in 2014 and 2016.[101] The amendments affected the Law on Information, Information Technologies and the Protection of Information, among many others, requiring the organizers of dissemination of information to notify Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass Media) of their activity as such so they can be included into the official registry of organizers of dissemination of information.[102]

Critics have argued that together with the overly broad definition of the organizer of dissemination of information, the new requirement could be arbitrarily applied to almost any individual to any legal entity who in some way provide electronic communications services to others in the country.[103] As such, any individual, any website or any online service that provides an opportunity for message exchange or commentary (i.e. dating websites, instant messengers, blogging platforms) could fall under the definition of the organizer of dissemination of information.[104]

Another troubling amendment introduced in 2016 required that the organizers of dissemination of information share upon request of the FSB the information necessary to decrypt any online

101 '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 17 October 2018
102 Decree of the Government of the Russian Federation of July 31, 2014 N 746
103 'Almost anyone can end up on the registry of Roskomnadzor' (Tinkoff Journal, 8 February 2018)< https://journal.tinkoff.ru/news/ori/> accessed 10 November 2019
104 Ibid

communications.[105] The amendment was justified as an additional measure necessary to strengthen the anti-terrorism efforts of the FSB and other national defense bodies.[106]

The Federal Law of 6 July 2016 on the amendment of the Federal Law on Counter-Terrorism (374-FZ), which puts forth such requirement, does not necessarily introduce new responsibilities for the organizers of dissemination of information regarding encryption, but rather sets out specific steps that the organizers must follow upon such a request on behalf of the authorities.

Critics of the amendments have argued that the new requirements were directed at establishing control over all electronic communications in order to be able to identify those that shared criticism of the government and actively expressed opposition to the Kremlin's politics.[107]

Soon after the amendments to the law were passed, the authorities asked the owner of the Russian messaging app, Telegram, to provide backdoors into the communications of its users to the FSB, relying on the amendments to the law and the new order by the FSB.[108] The fact that it happened soon after the amendments were passed suggests they were drafted intentionally with the aim of providing strong legal grounds to obtain the encryption keys from one of the most widely used messaging apps in Russia.[109]

[105] The author's own brief translation of the text of the amendment of the Federal Law on Counter-Terrorism (374-FZ)
[106] '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 17 October 2018
[107] 'Almost anyone can end up on the registry of Roskomnadzor' (Tinkoff Journal, 8 February 2018)< https://journal.tinkoff.ru/news/ori/> accessed 10 November 2019
[108] 'Telegram CEO Durov Says Russia's FSB Demands Messenger's Encryption Keys' (RFE/RL, 27 September 2017)<https://www.rferl.org/a/telegram-durov-russia-fsb-encryption-keys-security/28760575.html> accessed 10 November 2019
[109] Ibid

The owner of the app did not provide backdoors into Telegram's communications arguing that the request was unconstitutional and would violate the privacy of its users, and that it is technically impossible to share encryption keys with others.[110]

In response to the refusal to provide ecryption keys, Roskomnadzor ordered Internet Service Providers (ISPs) in Russia to block the messenger and imposed a fine on Telegram in the amount of eight hundred thousand rubles (approximately EUR 11,000).[111]

The case of Telegram has so far been the only precedent in Russia when the authorities attempted to block the service as a response to the refusal to comply with the law. However, it has sparked a lot of attention and action on behalf of privacy and internet freedom activists in Russia. A campaign called "The Battle for Telegram" was launched by Roskomsvoboda, a Russian NGO working for protection and promotion of digital rights in Russia.[112] The organization has become especially active following the passing of the said amendments.

As part of the campaign, and after the Supreme Court of Russia rejected a lawsuit filed by Telegram against the FSB, 35 activists submitted a collective complaint to the Court in Moscow, alleging that the recent requirements by the FSB to obtain encryption keys without judicial warrant violate Russian citizens' rights to inviolability of private life, privacy of correspondence, of telephone conversations,

110 Ibid
111 'The Battle for Telegram moves to Strasbourg' (Roskomsvoboda, 3 July 2019) <https://roskomsvoboda.org/47943/> accessed 10 November 2019 (in Russian)
112 Ibid

postal, telegraph and other messages, and the right to freedom of ideas and speech, as guaranteed by the Russian Constitution, Articles 23 and Article 29 respectively.[113]

The complaint was rejected by the Court on the grounds that since Telegram has not shared the encryption keys with the FSB, there was not violation of the complainants' rights.[114] The Supreme Court of Russia agreed and the case went to the European Court of Human Rights where it is currently under review.[115]

The overall position of the courts was that the obligation to disclose encryption keys does not violate the rights of the users of online communication providers to privacy, free speech and private correspondence, arguing that the constitutional protections do not extend to encryption keys.[116] As such, the Russian courts place encryption technologies outside of reach of constitutional protections, while creating restrictive laws which effectively prohibit the secrecy of private communications to the Russian citizens. Such position underscores the existing gap between the Russian law and constitutional guarantees, which does not just weaken constitutional guarantees but undermines the very values which the document is meant to protect.

However, as the Russian activists await the development of the case at the ECtHR, the enforcement of the law still leaves a lot of questions about feasibility of its technical and legal implementation. Analogous to the Apple's security system, Telegram does not have access to the keys used to encrypt the communications of the messenger's users, as the keys are generated on their devices and the Telegram's team does not have them to share with the FSB.[117] As such, even if Telegram wanted to comply with the

[113] Ibid
[114] Ibid
[115] Ibid
[116] Ibid
[117] 'Secret Chats' (Telegram) <https://telegram.org/faq#secret-chats> accessed 11 November 2019

order of the FSB, it would not be able to provide the desired encryption keys to them. The Russian authorities are asking for something which is impossible, according to the way that the Telegram's security system works, in the same manner that the US Court requested Apple to provide backdoors into the iPhone. This is another example that showcases a huge gap in lawmakers' understanding of technology and the detrimental effects such laws might have on the exercise of human rights in the digital age.

The Telegram case suggests the ineffectiveness of the law and the inability of the Russian law enforcement to implement the law on the technical level. Nevertheless, it can be argued that the recent Russian counterterrorism laws pose significant challenges not only for the right to privacy and freedom of expression, but also for carrying out human rights work which depend on the exercise of these rights.

The individuals behind the collective complaint are activists, journalists, lawyers and IT-specialists, for whom the protection of private communication is not just a personal issue but also a professional responsibility.[118] The activists at Roskomsvoboda believe the case is a potential precedent for the ECtHR which is likely to receive more cases dealing with encryption restrictions and bans from the countries under its jurisdiction.[119]

In Russia, the civil society and human rights actors seem to be the main targets of the recent legislations imposing restrictions on the use of encryption technologies in the country. Telegram is being used widely by the Russian users, and its encryption function allows its users to easily protect the content of their

[118] 'The Battle for Telegram moves to Strasbourg' (Roskomsvoboda, 3 July 2019) <https://roskomsvoboda.org/47943/> accessed 10 November 2019 (in Russian)
[119] Ibid

private communications by enabling secret chats, which are end-to-end encrypted, and the contents of which are only available to the intended recipients.

In a country where the recent years have been marked by an increase in censorship laws, security of private communications, protection of private information and private life, the ability to freely express and share a dissenting view has become more important than ever. Apart from other services that offer anonymity and secure communications, such as VPNs and encryption programs for email, instant messaging apps such as Telegram remain go-to tools for activists, journalists, human rights advocates and ordinary citizens concerned about their right to privacy and the broadening scope of laws that aim to curb it.

Jurisdiction 2 – Turkey

In 2016, immediately following a coup attempt, Turkey declared a nationwide state of emergency, which lasted until July 2018.[120] The two years marked a rapid increase in arrests and persecutions of activists, journalists, academics and ordinary citizens on the suspicion of belonging to a terrorist group blamed for staging the coup.[121] It was in the context of the state of emergency that Turkey accused 50,000 Turkish citizens for downloading and alleged use of ByLock, an encrypted messenger.[122] The mere fact of possession of ByLock represented legal grounds for an allegation that its users were a part of the Gulenist movement allegedly behind the coup.[123]

120 'Turkey ends state of emergency after two years' (BBC, 18 July 2018) <https://www.bbc.com/news/world-europe-44881328> accessed 19 October 2018
121 'We need to talk about Turkey,' (Amnesty International) https://www.amnesty.org/en/latest/campaigns/2018/04/turkey-human-rights-defenders-under-attack/ accessed 18 October 2018
122 'Freedom on the Net 2018, Report, Turkey' (Freedom House) <https://freedomhouse.org/report/freedom-net/2018/turkey> accessed 3 October 2018
123 Ibid

The leading organizations working for protection and promotion of free expression and free Internet expressed mounting concern with the Turkish prosecutors basing their allegations on the mere possession of the encrypted messaging app.[124] The statement said, "As many as 50,000 people were arbitrarily detained with the use or download of the encrypted ByLock app given the as evidence, and many thousands more dismissed or subject to disciplinary procedure on the same grounds."[125]

The arbitrary arrests of thousands of Turkish citizens for using ByLock, and the allegations that it was used by the members of the Gulenist movement to plot the coup, strengthened the anti-encryption narrative suggesting public access to encryption poses danger to national security and public safety. In the context of the coup, it almost equated the use of encryption to a terrorist act.

Because the state of emergency was declared following the attempted coup, the limitations to the exercise of most rights, including the right to freedom of speech, the right to private life and the right to communication, were in effect,[126] which led to an unprecedented crackdown on civil society, as will be illustrated further.

[124] Joint submission to the Universal Periodic Review of Turkey by Article 19, P24, PEN International, English PEN, Reporters Sans Frontiers (RSF), International Press Institute (IPI), Freemuse, European Centre for Press and Media Freedom (ECPMF), IFEX and Norsk PEN, July 2019. Para. 38

[125] Ibid

[126] Information note on the decree-law No. 699 of 31 July 2016 on the measures taken under the state of emergency

A group of eight human rights activists and two digital security consultants, also known as the Istanbul 10, were detained on July 2017.[127] The human rights defenders and trainers faced terror-related charges and spent four months in detention[128] for participating in a holistic security workshop, which covered digital security tools and strategies, including encryption.

Turkey's constitution provides elaborate protections for privacy, freedom of expression, opinion and thoughts, and even freedom of communication. For the purpose of this essay, an official translation of the Turkish Constitution into English will be used. Chapter II of the Turkish Constitution is dedicated to "fundamental rights and duties." Article 20, part IV (A), "Privacy and protection of private life," states, "Everyone has the right to demand respect or his/her private and family life. Privacy of private or family life shall not be violated."[129] Article 22, Part C, "Freedom of communication" provides that "Everyone has the freedom of communication. Privacy of communication is fundamental."[130] Part VII, "Freedom of thought and opinion," Article 25 states: "No one shall be compelled to reveal his/her thoughts and opinions for any reason or purpose; nor shall anyone be blamed or accused because of his/her thoughts and opinions."[131] In Part VIII "Freedom of expression and dissemination of thoughts," Article 26 provides:

> Everyone has *the right to express and disseminate his/her thoughts and opinions* by speech, in writing or in pictures or *through other media,* individually or collectively. This freedom includes

[127] 'Ten Human Rights Defenders Detained in Turkey' (Front Line Defenders, 5 July 2017) < https://www.frontlinedefenders.org/en/profile/ten-human-rights-defenders-detained-turkey> accessed 18 October 2018
[128] 'Istanbul 10 Released' (Front Line Defenders, 25 October 2017) <https://www.frontlinedefenders.org/en/case/istanbul-10-released-turkey> accessed 18 October 2018
[129] The Constitution of the Republic of Turkey, Article 20, part IV (A)
[130] Ibid, Article 22 (C)
[131] Ibid, Article 25

> *the liberty of receiving or imparting information or ideas without interference by official authorities*. ***This provision shall not preclude subjecting transmission by radio, television, cinema, or similar means to a system of licensing.***[132] [emphasis added]

Except for Article 25, "Freedom of thought and opinion," all abovementioned rights have an elaborate restriction clause, which, with slight variation, provides the following justifications: "national security, public order, prevention of crime, protection of public health and morals or protection of the rights and freedoms of others, …. a written order of an agency authorized by law."[133] The restriction for the right to freedom of expression and dissemination of thought is phrased more elaborately and includes:

> national security, public order, public safety, ***safeguarding the basic characteristics of the Republic and the indivisible integrity of the State with its territory and nation*** [emphasis added**]**, preventing crime, punishing offenders, withholding information duly classified as a state secret, protecting the reputation or rights and private and family life of others, or protecting professional secrets as prescribed by law, or ensuring the proper functioning of the judiciary.[134]

When comparing the two Articles in the Turkish Constitution, Article 25 "Freedom of thought and opinion" and Article 26 "Freedom of expression and dissemination of thought," one can conclude that the drafters of the constitution made an explicit and hence conscious distinction between the two rights - while

[132] Ibid, Article 26
[133] The Constitution of the Republic of Turkey, Articles 20, 22, 26
[134] Ibid, Article 26

an individual's right to have thoughts and opinions is absolute, as there is no restriction of any sort provided in the text of the constitution for this right, the right to freedom to disseminate that thought and opinion is subject to restriction. In making such distinction, the Turkish constitution is in line with the international standards, such as ICCPR, and does not merit criticism, at first glance.

It is important to assess the relevant legislation governing the use of cryptographic technology in Turkey. All communications that take place in digital spaces are governed by the Electronic Communications Law of 2006. The law establishes a set of rules for the operation of electronic communications services in the country, outlines responsibilities associated with the operation of such services to their providers and prescribes penalties and fines for failing to comply with provisions of the law.

The law establishes that the Information and Communication Technology Authority (also the ICTA or the Authority) conducts oversight over all matters concerning the operation of communication technology in the country.[135] The law basically requires all electronic communications services to be authorized for operating in the country, stating that "authorization for the installation and operation of any kind of electronic communications equipments, systems and networks" should be done in accordance with certain principles set out in the law.[136]

A long list of principles follows in the text of the law targeting a wide range of areas from "development plans" and "free and efficient competitive environment" to "… implementation of technological innovations."[137] Two principles are specifically worth noting – "giving priority to the requirements of

[135] Electronic Communications Law, Article 1
[136] Electronic Communications Law, Article 4 – (1)
[137] Electronic Communications Law, Article 4 – (1)

national security, public order and emergency situations" and "protection of information safety and confidentiality of communication."[138] The latter principle directly references Article 22, Part C, "Freedom of communication," which guarantees freedom of communication to everyone and proclaims privacy of communication to be fundamental.[139]

The latter is the very last principle on the list. It is hence logical that in light of existing restrictions on the exercise of the right to privacy and the right to free speech articulated in the Turkish Constitution, among the two principles one will always prevail – namely, the priority of national security and public order over safety and confidentiality of communications.

By making an emphasis on national security and public order and explicitly referencing emergency situations in the part of the law[140] which sets out a base for its application, the Turkish lawmakers deem the rights to communication and privacy of second importance.

There are also several provisions in the law that provide a lot of leeway to the authorities who oversee the operations of electronic communication services. First such provision, i) under Article 6 – (1) "Competencies of the Authority" states that the Authority can:

> … request any kind of information and documents from the operators, public authorities and institutions, natural persons and legal entities which deemed necessary pertaining to electronic communications and to keep necessary records, to present those needed to the Ministry upon

[138] Electronic Communications Law, Article 4 – (h), (l)
[139] The Constitution of the Republic of Turkey, Article 22
[140] Ibid, Article 4 – (h)

request in determination of the strategies and policies towards electronic communications sector.[141]

Such a provision should be considered problematic from the standpoint of the application of the law. Not only does it raise clarifying questions regarding the type of information and documents that the Authority may request, but also about the meaning behind "strategies and policies towards electronic communications sector." In what situation can the authority request such information and how will the strategies and policies towards the sector be shaped in the future? These and many other questions come to mind upon evaluation of the given provision. In short, the law, including this provision, entrusts the Authority with a broad range of competencies which can be exercised in almost any situation.

In addition, the Authority is entrusted with taking "… measures specified by the legislation with a view to ensure that the national security, public order or public service are duly maintained in electronic communications sector."[142]

It is important to note that there is a leeway already deliberately placed in the text of the Turkish Constitution allowing for the rules and restrictions prescribed by the Law. Apart from guaranteeing freedom to express, impart and receive information, Article 26 states that "This provision shall not preclude subjecting transmission by radio, television, cinema, or similar means to a system of licensing."[143]

When it comes to encryption, in Turkey, regulations on the use and application of cryptographic technologies are also articulated in the Electronic Communications Law. Any equipment that enables

141 Ibid, Article 6 – (1) "Competencies of the Authority" (i)
142 Ibid, Article 6 – (1) "Competencies of the Authority" (s)
143 Constitution of the Republic of Turkey, Article 26

cryptographic and coded communications requires licensing.[144] Article 39 of the law titled "Cryptographic and coded communications" states:

> Turkish Armed Forces, General Command of Gendarmerie, Coast Guard Command, National Intelligence Organization, Security General Directorate and Ministry of Foreign Affairs are authorized to make cryptographic communications by radio communications systems. Procedures and principles for making coded and cryptographic communications in electronic communications service of public institutions and organizations except from those which are under the body of above-mentioned institutions and natural and legal persons shall be determined by the Authority.[145]

As such, the law only gives explicit authorization for the use of cryptographic technologies to the governing bodies directly implicated in the matters of national security. When it comes to ordinary users, the law leaves them under the oversight of the Authority, without explicitly stating what those regulations are.

In light of the arrests associated with the use of ByLock, a question regarding the operation of messaging apps comes to mind: are encrypted messaging apps such as WhatsApp, Signal or ByLock authorized under the given law? Do ordinary users have to get approval for their use from the Authority? Does the authority provide specific steps, if any, to be taken by ordinary users to comply with the regulation if they use encrypted communication services?

[144] Constitution of the Republic of Turkey, Article 39
[145] Ibid

The law does not provide an explicit answer to those questions. The provisions that can give some level of insight into how the use of encrypted electronic communication services by ordinary persons is governed under the law are just a few. The law states:

> …electronic communications service and/or the network or infrastructure shall not be subject to authorizations, which is;
>
> a) Within any natural person's or legal entity's property under his/its own use, which does not exceed any property's borders, which is used upon exclusively individual or organizational needs, which is not used for providing any electronic communications services to third parties, which is provided without any commercial intention and which is not publicly available…[146]

If formulated as such, the use of a messaging app for personal use does not fall within the category of the types of electronic communication services that should be licensed. Neither is cryptographic function of such communication services specifically mentioned in the law.

However, cryptographic technology is mentioned once again in Chapter Seven of the law on penal provisions. Article 63 – (6) states:

> Perpetrators who communicate by means of coded and cryptographic communication or who enable such communication in defiance of Article 39 of this Law shall be punished by judicial fine from five hundred days to one thousand days.[147]

[146] Electronic Communications Law, Article 8 –(2(a))
[147] Electronic Communications Law, Article 63- (6)

In laying out penalties for the use of coded and cryptographic communication, the text of the law circles back to Article 39 which entitles the national security and defense bodies to use the said technology, while leaving ordinary individuals under discretion of the Authority, for which the law does not provide specific rules. Moreover, the law uses the word "perpetrator," and does not differentiate between governmental bodies, organizations and natural persons. The latter, for example, is exempt from the responsibility to obtain a license to use electronic communication services for personal use. The law therefore leaves the definition of "the perpetrator" extremely vague, leaving a lot of room for the authorities to apply the provision to almost anyone.

Under this law, the provisions of the Constitution that guarantee the rights to privacy and free expression can be downplayed due to the emphasis on national security and due to unlimited reach of power and control allocated to the governing bodies. It can be argued that any individual or legal entity could be found in violation of the law for the use of encrypted messaging apps or other communication services such as emails or encrypted video chats. This law also makes it easy to derogate from the international human rights norms inscribed in ECHR and ICCPR, to both of which Turkey is a State Party.

As in many other jurisdictions, and in line with restrictions provided for in ECHR and ICCPR, the Turkish government may interfere with, interrupt or shut down the services of the providers of electronic communications in case there is an ongoing criminal investigation pursuant by the order of the judge or in case if national security and public order are threatened and for protection of public health and public morals or of the rights and freedoms of others. [148]

[148] 'Telecoms privacy and data security provisions in Turkey,' Esin Attorney Partnership. (LEXOLOGY, 5 October, 2018)< https://www.lexology.com/library/detail.aspx?g=cfb4eba8-cc01-4b09-acf3-41a8c7b3d962> accessed 5 November 2019

Upon declaring the state of emergency following the attempted coup in 2016, the authorities arrested around 50,000 people, resulting in mass arrests of activists, journalists, academics, writers and basically concerned citizens with a critical perspective on the government of Turkey.[149] On the one hand, the attempted coup could serve as a justification for prosecution of many people as part of the investigation into the plot. On the other hand, as the number of arrests was growing and the prosecution turned into persecution of masses, it was only logical to assume that a large crackdown on the civil society, free speech and dissenting views was underway in Turkey.[150]

Experts note that the use of encryption has been mentioned as an offence in an overwhelming number of cases of those arrested in the aftermath of the coup.[151] However, it can be argued that in this scenario it was not the encryption per se that the authorities went after but rather that the authorities considered the use of encryption in the context of the attempted coup as a reason for making more arrests. Regardless, encryption was criminalized in the context of the state of emergency in Turkey.

The case of the Istanbul10 has underscored the arbitrary and overreaching nature of the persecution that took place in the country. A group of eight human rights defenders and two digital security consultants were detained on 5 July 2017.[152] The group included Turkish activists working for human rights organizations such as the Helsinki Citizen's Assembly, Amnesty international Turkey, Human Rights Agenda Association, Women's Coalition and the Association for Monitoring Equal Rights.[153] All were

[149] Joint submission to the Universal Periodic Review of Turkey by Article 19, P24, PEN International, English PEN, Reporters Sans Frontiers (RSF), International Press Institute (IPI), Freemuse, European Centre for Press and Media Freedom (ECPMF), IFEX and Norsk PEN, July 2019. Para. 38
[150] Ibid
[151] Ibid
[152] 'Ten Human Rights Defenders Detained in Turkey' (Front Line Defenders, 5 July 2017) < https://www.frontlinedefenders.org/en/profile/ten-human-rights-defenders-detained-turkey> accessed 18 October 2018
[153] Ibid

charged with "aiding armed terrorist organization"[154] for participating in a holistic security workshop, which covered digital security tools and strategies, including encryption.

The case of Istanbul 10 supports the assumption that the persecution of the civil society actors has only increased during the state of emergency, and that encryption, its widely spread use among human rights actors and civil society, has been perceived as a threat to the status quo of the government and something that has to be regulated.

Comparative analysis of jurisdictions

In this section the author will conduct comparative analysis of the jurisdictions in the context of the international human rights law.

Following the overview of the Turkish and Russian jurisdictions, specifically the laws that govern the use of encryption technologies, the author aims to compare the two countries with the aim of drawing parallels and distinctions in the legislative approach to the encryption technology in the given countries.

Both Turkey and Russia are state parties to the ECHR and ICCPR, two major international human rights mechanisms, which set the standard for human rights norms and protections for those norms in the states that are parties to the given conventions. Since the main focus of this essay are the rights to privacy and freedom of expression, only the provisions relevant to the said rights were considered for this analysis.

[154] 'Istanbul 10 Released' (Front Line Defenders, 25 October 2017) <https://www.frontlinedefenders.org/en/case/istanbul-10-released-turkey> accessed 18 October 2018

Based on the analysis of the provisions in the Russian and Turkish Constitutions, there are well-spelled guarantees for the rights to privacy and freedom of speech in both countries. Both Constitutions offer protections to private and family life, inviolability of home and private correspondence.[155]

The Turkish constitution makes an emphasis on "freedom of communication," stating that "…privacy of communication is fundamental."[156] It also guarantees that individuals can't be compelled "to reveal his/her thoughts and opinions for any reason or purpose; nor shall anyone be blamed or accused because of his/her thoughts and opinions."[157]

The Russian Constitution is less elaborate when it comes to freedom of expression and states "everyone shall be guaranteed freedom of ideas and speech."[158] However, the Russian Constitution is more elaborate than the Turkish in specifying protections for private conversations, detailing the privacy "of correspondence, of telephone conversations, postal, telegraph and other messages."[159]

While the Turkish Constitution has more emphasis on the right to free speech, the Russian Constitution is more elaborate on the concept of privacy. Nevertheless, both documents reflect full well the norms articulated in the international human rights documents such as ICCPR and ECHR. As such, the constitutions reflect the rationales for both, the right to privacy and the right to free expression, especially from the perspective of one's autonomy with regards to how their communications, private information

[155] The Constitution of the Russian Federation, Article 23; The Constitution of the Republic of Turkey, Article 22
[156] The Constitution of the Republic of Turkey, Article 22
[157] The Constitution of the Republic of Turkey, Article 25
[158] The Constitution of the Russian Federation, Article 29
[159] Ibid, Article 23

and secretes are being handled. The fact that the constitutions acknowledge ideas, thoughts and opinions as assets that need to be protected, whether on their own or as contents of communications, underscores their value in the given legal systems, at least from the theoretical point of view.

However, when it comes to the acting legislation analyzed in previous sections, there seems to be a contradiction between the protections offered in the Constitutions and the laws that directly have effect on the exercise of freedom of expression and the right to privacy. The laws in question are the Turkish Electronic Communications Law and the Russian Federal Law on Information, Information Technologies and the Protection of Information. Both laws govern electronic communications and as such provide regulations on the use of cryptographic technology. Both laws recognize that the cryptographic technology requires some extent of regulations that allow the authorities to have control over such technologies and the content of communications, if necessary. Both laws recognize that certain governing bodies, such as defense ministries and security services, as well as state information systems can use such technology in their own activities and communications.[160]

The laws are also similar in their approach to the use of electronic communication services by individuals. In Turkey, the law on electronic communications states that individuals do not have to obtain authorization for the use of electronic communications services if such services are used for the personal needs of individual, are not used with any commercial intention and are not available to the public.[161] Similarly, in

[160] Federal Law No. 149-FZ of July 27, 2006 on Information, Information Technologies and the Protection of Information, Article 10.1.1; Electronic Communications Law, Article 39
[161] Electronic Communications Law, Article 8 – (2(a))

Russia, the law does not require individuals who use electronic communication services for personal and family needs to obtain license for its use.[162]

However, when it comes to the use of electronic communication services by individuals neither law has specific regulations for the use of encryption. In the Turkish law, use of encryption by an individual is only implied under Article 63 – (6) which lays out penalties for "perpetrators who communicate by means of coded and cryptographic communication or who enable such communication in defiance of Article 39."[163] As such, the Turkish law does not provide an elaborate regulation on the use of encrypted communications by ordinary persons. Moreover, it recognizes that electronic communications providers do not have to be authorized if they are used for personal purposes. Nevertheless, the law has an elaborate provision on penalties in case cryptographic technology is used in a criminal act or act of terrorism. The law does not specify what kind of crime should be committed for an individual to be penalized, but the vague formulation of the provision leaves a lot of space for interpretation and allows space for its application without acknowledging the distinctions between institutions and governing bodies and individuals.

Therefore, in Turkey, if an individual is prosecuted as a perpetrator of a crime, a judicial warrant is necessary to receive access to one's communications. If such procedure is followed, then the law does not violate the Constitution. However, even if the procedure is followed, but the grounds for it are questionable, then there is an assumption that the judicial authorities have exceed their instructions and the question of fairness and legality of such procedure is raised.

[162] The Federal Law No. 149-FZ of July 27, 2006 on information, information technologies and the protection of information, Article 10.1.5
[163] Electronic Communications Law, Article 63 – (6)

This can be illustrated with the case of one of the activists of the Istanbul 10, Tener Kilic, the Chair of Amnesty International Turkey. According to Front Line Defenders, an international NGO working to protect human rights defenders at risk, which reported on the proceedings of the arrested activists, the charges against Kilic were based on the anonymous testimony of a witness claiming they overheard "allegedly incriminating conversations."[164] Kilic was also one of the people who were arrested on the basis of the alleged downloading of ByLock and charged with "membership of an armed terrorist organization."[165] As none of the accusations could be proven, Kilic was finally released after spending more than a year in detention.[166]

The case of Kilic, as well as tens of thousands of other cases of individuals who have been suspected of belonging to a terrorist organization, the Gulenist movement, which was believed to be behind the coup, is a perfect example of how the state of emergency can lead to a disregard of the constitutional protections for human rights and the rules of the legal proceedings.

On August 5, 2016, following declaration of a country-wide state of emergency in July of the same year, Turkey submitted a communication to the Secretariat General of the Council of Europe explaining the nature of measures taken under the state of emergency.[167] According to the communication, the measures

[164] 'Taner Kilic Released' (Front Line Defenders, 16 August 2018) <https://www.frontlinedefenders.org/en/case/istanbul-10-released-turkey#case-update-id-6815> accessed 5 November 2019

[165] Ibid

[166] Ibid

[167] Reservations and Declarations for Treaty No. 005 – Convention for the Protection of Human Rights and Fundamental Freedoms. Communication transmitted by the Permanent Representative of Turkey and registered by the Secretariat General on 5 August 2016, Council of Europe, available at: https://www.coe.int/en/web/conventions

were justified "for the purpose of effective fight against the FETÖ terrorist organization."[168] It also stated that the declaration of the state of emergency was necessary for "protecting the rule of law, democracy and human rights by way of removing the members of the FETÖ terrorist organization from the State's institutions."[169] The note also stated that "no restriction was brought on the rights and freedoms of the public with the Decree-law."[170]

Contrary to the statement in the note that the measures under the state of emergency were directed at the military and state institutions, an overwhelming number of those arrested did not have any connection with those bodies. Among the arrested were writers, journalists, human rights activists and even foreigners,[171] all of whom were also charged with aiding a terrorist organization or being a member of a terrorist organization. [172]

The scope of the crackdown on the civil society that took place throughout the duration of the state of emergency indicated that the Turkish government has exceeded its authority under Article 15 of ECHR "Derogation in time of emergency," which provides that s state party can derogate from its obligations under the Convention "in the extent strictly required by the exigencies of the situation."[173] A conclusion can be made that the Turkish government surpassed its own justifications as laid out in the explanatory note presented to the Council of Europe.

[168] Information note on the decree-law No. 699 of 31 July 2016 on the measures taken under the state of emergency
[169] Ibid
[170] Ibid
[171] Among the 10 human rights activists who were arrested on 6 July 2017, also known as Istanbul 10, there were two foreigners – German national Peter Steudtner and Swiss national Ali Gharavi, both digital security consultants.
[172] Joint submission to the Universal Periodic Review of Turkey by Article 19, P24, PEN International, English PEN, Reporters Sans Frontiers (RSF), International Press Institute (IPI), Freemuse, European Centre for Press and Media Freedom (ECPMF), IFEX and Norsk PEN, July 2019. Para. 38
[173] ECHR, Article 15

While in Turkey the authorities can rely on the provision in the law that defines penalty for the use of encryption by perpetrators of a crime,[174] in Russia, the law is written in a way that the organizers of dissemination of information are obligated by the law to provide the information necessary for the state to get access to one's communications without a judicial warrant.[175]

In Russia, the use of encrypted communications is not regulated by the law on the level of an individual user. Instead, the law targets organizers of dissemination of information by requiring them to register as such with Roskomnadzor and therefore be potentially obliged to disclose all the necessary information for decrypting electronic communications of their users. Instead of going directly after individual users and restricting their use of encrypted electronic communication services, the Russian authorities pursue the providers of such communications, and therefore indirectly restrict the right to private correspondence of the Russian users.

In Russia, the amended law now allows FSB to request access to individual's communication without a warrant, which is in direct violation of the second part of Article 23 of the Russian Constitution, stating that the limitations on "the right to privacy of correspondence, of telephone communications, postal, telegraph or other messages… shall be allowed only by court decision."[176]

[174] The Constitution of the Republic of Turkey, Article 63 - 3
[175] Federal Law No. 149-FZ of July 27, 2006 on Information, Information Technologies and the Protection of Information, Article 10

[176] The Constitution of the Russian Federation, Article 23 (2)

It is concerning that the Russian government has issued such amendments in the context of anti-terrorism and anti-extremism measures. Such a move signifies that the authorities equate the use of encryption in any kind of communications, especially those of private users, as potentially posing risk to the national security, sovereignty and integrity of the state.

In the midst of the crackdown on Telegram, a controversial case developed in Russia in which a group of teenagers was accused of plotting to overthrow the Russian government using Telegram's encrypted chat.[177] As the case was developing, the investigative journalists of Russia's independent newspaper Novaya Gazeta uncovered connections between several of the chat's participants and the FSB, concluding that the informants were actively engaged with the group and even took leadership in organizing meetings and producing so-called "extremist" materials, such as the group's charter.[178]

As the case remains under review, it follows based on the investigations of the independent media that the case of the extremist movement called "Novoe Velichie" (New Greatness) was carefully built with the help of the FSB informants with the aim of creating a precedent that would legitimize the application of the amended law requiring providers of encrypted electronic communications to share encryption keys with FSB.[179]

177 'Another police informant emerges in a controversial case against an alleged Russian extremist group' (*Meduza*, 3 July 2018) <https://meduza.io/en/news/2018/08/27/another-police-informant-emerges-in-a-controversial-case-against-an-alleged-russian-extremist-group> accessed 9 April 2019

178 'Podsadnye kukly' (Novaya Gazeta, 27 August 2018) <https://novayagazeta.ru/articles/2018/08/26/77605-podsadnye-kukly> accessed 6 November 2019 (in Russian)

179 Ibid

If FSB indeed put so many resources into fabricating a case to be used as a precedent for the law's application, how are such actions legitimate and is there a real threat posed to the national security of the state by Telegram's secret chats? The answer suggested by the available information is "no." Even if in theory, the wide-spread availability of encryption potentially poses danger to national security and public order as it can be used by criminals and terrorists, only the "Novoe Velichie" case has so far received so much attention and such a wide-spread coverage in the Russian media.[180]

This case shows that the application of the Russian law is selective and arbitrary. It also suggests that the justification for the amendments to the law are far-fetched and raise questions as to the necessity of the proposed requirements. In addition, it suggests another reason for which such amendments could have been passed, namely – to allow the authorities to control private communications of citizens with the aim of censoring the expression which can be deemed dangerous and threatening to the Russian government.

In 2013 The General Assembly adopted a resolution on the right to privacy in the digital age, which recognized that human rights should be protected equally online and offline. [181] The resolution called upon states:

a) To respect and protect the right to privacy, including in the context of digital communication;
b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by *ensuring that relevant national legislation complies with their obligations under international human rights law*. [emphasis added][182]

[180] Ibid
[181] United Nations, General Assembly, Resolution adopted by the General Assembly on 18 December 2013, The right to privacy in the digital age, A/RES/68/167, para 3
[182] Ibid, para 4 (a), (b)

Although a General Assembly is not binding by itself, it offers an authoritative interpretation of the way that the international human rights law should be complied with by the States that are bound by it. As such, the recommendations spelled in the resolution should have been followed by both Russia and Turkey in shaping their domestic legislation that governs digital communications. To the contrary, however, both states have expressed disregard to the norms inscribed in the international human rights law, both ICCPR and ECHR.

Discussion of themes and recommendations

The analysis of the laws governing the use of electronic communications and cryptographic technology suggests a number of common themes that emerge from the reviewed case-studies of Turkey and Russia. The main overarching theme that can be traced throughout the analysis of both Russian and Turkish case-studies is the justification for anti-encryption legislation as an anti-terrorism measure. While in Russia the controversial legislation requiring the organizers of dissemination of information to share encryption keys with the state security services was passed in the context of strengthening the anti-terrorism efforts, Turkey used the already existing law during the state of emergency as a means for arresting the alleged members of a terrorist organization that was blamed for plotting the coup.

This is a reflection of a wider trend among some states, both democratic and non-democratic, to push for stricter regulations on encryption.[183] In doing so, these states are guided by belief that the advancement of

[183] 'The international encryption debate: privacy versus big brother' (LEXOLOGY, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 3 September 2019

technologies, including the increase in wide-spread usage of encrypted communications, poses a significant challenge to the ability of law enforcement agencies to prevent crime and terrorism acts.[184] A prominent examples of such a perspective is the Apple V FBI case, which has exposed the strengths of both arguments in the privacy versus security debate.

In December 2015 a shooting in San Bernardino took lives of 14 people, and the FBI turned to Apple in the course of the investigation to gain access to the iPhone belonging to one of the shooters.[185] Apple refused to comply with the request arguing that the company could not provide the backdoors into the iPhone for two reasons – first, it was technically impossible; second, it would compromise the security system of Apple's products which was designed by default to protect users' privacy.[186] The answer of Apple reflects the other side of the debate – the argument for privacy and for encryption as its main enabler.

It could be argued that the rise in use of cryptographic technologies, such as instant messengers with encrypted chats, encryption software for email and VPNs (Virtual Private Networks allowing users to browse the webpages anonymously), can be attributed to the increase in awareness among Internet users about mechanisms of surveillance and data gathering conducted by both states and non-state actors, especially large corporations and tech companies.[187] It is only logical for the users of the Internet to want to protect their data and communications from the all-encompassing surveillance of tech-giants and

[184] Ibid
[185] 'San Bernardino shooting: what we know so far' (BBC, 11 December 2015)< https://www.bbc.com/news/world-us-canada-34993344> accessed 10 October 2019
[186] 'A Message to Our Customers' (Apple, 16 February 2016) <https://www.apple.com/customer-letter/> accessed 11 October 2019
[187] Surveillance giants: how the business model of Facebook and Google threatens human, Amnesty International Report, 2019, pp. 12-13

businesses that want to build profit using their data. After in 2013 Edward Snowden revealed the existence of a pervasive surveillance system that targeted communications of both Americans and foreign citizens,[188] a concern about privacy, personal data and, as a result, an interest towards privacy-enhancing technologies grew tremendously.[189] It can be argued that the growing usage of encrypted technologies has more connection to the public concern over privacy rather than a sudden flourishing of terrorism and criminal activity hidden behind it. This is not to deny the fact that criminals and terrorists are as likely to use encryption in their communications as an ordinary citizen concerned about his or her privacy. However, the likelihood of such a scenario should not outweigh the argument for privacy. So far, the argument for security often wins over the argument for privacy, which is reflected in the law-making practices of some countries, such as Russia, for example.

The second theme is the lack of understanding on behalf of the governments about how to control encryption technology used by ordinary citizens. Both examples of Russia and Turkey show that there are well-spelled regulations on the use of encryption for the state bodies; the gap emerges when it comes to the use of encryption in private communications of ordinary citizens. While in Russia, private communications of individuals can be scrutinized by the authorities by way of requesting encryption keys from the communication service providers, in Turkey there is no specific regulation that would be used to get access to the contents of individual communications, except for a judicial warrant in case of criminal proceedings. Nevertheless, during the declared state of emergency, Turkish authorities have accused

[188] 'Edward Snowden: the whistleblower behind the NSA surveillance revelations' (The Guardian, 11 June 2013) <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> accessed 15 November 2019

[189] Edward Snowden: 'The people are still powerless, but now they're aware' (The Guardian, 4 June 2018) <https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware> accessed 15 November 2019

thousands of people of belonging to a terrorist organization solely on the basis of downloading an encrypted messaging app. It can be argued that by doing so the Turkish authorities were not concerned with the content of the communications as much as they were concerned with the fact that an encrypted app was so widely used in the midst of a political crisis.

The large-scale crackdown on the civil society was a direct result of the inability of Turkish government to control the sharing and free flow of information and the subsequent fear that information and ideas can spread widely and securely with the help of cryptographic technologies.

Drawing on the emblematic example of the Apple VS FBI dispute, it can be seen that even in a democratic state where individuals enjoy strong constitutional protections, it is not hard to build a case against the use of encryption based on the national security argument. However, in non-democratic states, the national security argument is more likely to outweigh the protections guaranteed to individuals under constitutional provisions. In states such as Turkey and Russia, despite the presence of strong constitutional protections on paper, the authorities abuse their law-making powers to get access to people's private communications and ignore their obligations under international human rights law. Such a situation underscores a troubling trend when some states abuse such important notions as national security and public order to bypass their obligations and restrict the rights and freedoms of their citizens.

National security and public safety are extremely important conditions that have been proven weak and easily shattered by many events in the course of history. Today, these notions are being abused by governments that want to tighten their grip over civil society, remain in power and protect their status quo. Turkey and Russia could be seen as examples of such abuse. The abuse of these notions for the sake of

keeping power devalues these important conditions of our society that were considered worthy of allowing certain derogations from the internationally recognized human rights norms. Before "national security" and "public safety" as concepts, as conditions of our society, stop being perceived as such, and become go-to excuses for infringement upon human rights in the digital age, it is important to balance out the values that both sides of the argument are built on. While it is important to recognize the crucial character of safety and security, it is also vital to understand the connection between privacy as a state of an individual which does not only allow for self-development and fulfillment, but as such is an essential aspect of a pluralist democratic society. If one considers a secure and safe state to be democratic, free of discrimination and equal for all its citizens, then privacy should be viewed as an essential element of such a state and therefore should be protected. From this standpoint, privacy and security are not be mutually exclusive, and should be viewed as interconnected and complementary to each other.

The third theme is directly connected with the second and indicates a big gap in lawmakers' understanding about how technology works. The demands by the FBI and FSB to obtain encryption keys from Apple and Telegram respectively could not be met for several major reasons. The first and foremost reason was privacy and unconstitutionality of the demands. However, even if the companies were compelled to disclose such information, it would have been technically impossible for either of them, since their security systems are built to not allow such interference.

This is a testament to the power behind encryption technology, its ability to protect and secure one's communications, speech and privacy. Had the Turkish and Russian governments have an option of breaking encryption, they would not have resorted to measures such as mass imprisonment or blocking of messenger's services.

As such, encryption is hard to control by law, primarily because of how cryptography works from the technical perspective. It is a common trend for the lawmakers and politicians to draft laws which are supposed to govern the use of highly sophisticated technology without sufficient understanding of how the technology really works. As a result, the implementation of such laws does not lead to intended results, but often leads to negative perceptions of technologies, such as encryption, as well as wrong understanding of how these technologies work and what they can be used for. The laws that are based on the assumption that encryption technology is being widely implicated into criminal activities and terrorism, are misleading not because such technologies are not being used by terrorists or criminals, but because such an approach does not leave any space for an argument in favor of such technologies. And by excluding the positive argument in favor of encryption technologies, the narrative automatically excludes human rights from the debate, leaving it entirely about collective safety and security and not about individual's freedoms and rights.

Following the discussion of the themes, the author will suggest several concrete recommendations based on the discussed challenges.

Frist, encryption should be recognized as a unique tool because of the enabling and protective values it carries for the exercise of human rights in digital spaces.

In its resolution on the right to privacy in the digital age, the United Nations General Assembly called upon states:

> To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;[190]

As encryption has become a tool for protection against surveillance of communications, collection of personal data and mass surveillance, it is being targeted for its protective function. In addition to the issues covered in the resolution, encryption should become the main focus for protection under international human rights law as a tool that has an enabling function for the exercise of a number of rights, particularly, but not limited to, the right to freedom of expression and the right to privacy.

Second, mandatory consultations with technologists and IT-specialists should become a requirement for any law-making process which directly concerns the use of technologies by the public. It is crucial that the perspectives of national security and human rights experts are equally represented and considered as part of any law-making process which will have direct implications for the exercise of human rights in online spaces.

Even though an argument can be made that it would be impossible to achieve the lawmaking process and advancement of technology to go hand-in-hand due to the rapid nature of such advancement, we should attempt to make any law-making process concerning the use of technologies as informed as possible with

[190] United Nations, General Assembly, Resolution adopted by the General Assembly on 18 December 2013, The right to privacy in the digital age, A/RES/68/167, para 4 (c)

the aim of avoiding the potential overreach on behalf of the authorities and creating wrong perceptions about the functions of these technologies.

Finally, the weakness of international framework for human rights protection necessitates special consideration for encryption as a tool for protection of the exercise of human rights online. If constitutional guarantees for the rights to freedom of speech and privacy can be easily bypassed by states invoking the notions of national security, then encryption, due to its protective and enabling functions, should be considered a right by itself which can be exercised by individuals as a measure to safeguard the rights and freedoms of people. It follows that due to its protective nature, the value of cryptographic technology is so high that it may deem special protection under international human rights law. This recommendation finds support in the work of scholars who make an argument that there should be "a right to encrypt."[191]

Conclusion

Encryption is an inseparable part in the conversation about human rights in the digital age. It has been called a "leading vehicle for online security" and a means for privacy protection.[192] The connection between encryption and privacy is ever-present in our life, especially when it comes to our daily communications. The exercise of the right to privacy was proclaimed "important for realization of the

[191] Plasencia, Adolfo & O'Reilly, Tim, 'Encryption as a human right', *Is the Universe a Hologram? Scientists Answer the Most Provocative Questions.* Cambridge: The MIT Press, 2017.
[192] United Nations, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression, David Kaye,* A/HRC/29/32 (22 May 2015)

rights to freedom of expression and to hold opinions without interference, and as one of the foundations of a democratic society."[193]

Such a vision has found proof in the texts of scholars studying privacy. Closely examined works of privacy scholars underscore the close connection between privacy and other rights, especially the right to free speech. They also emphasize the importance of privacy as a key pre-condition for self-development, pluralism and democracy.

A more challenging, but equally important insight into privacy speaks about its constantly changing nature, to a large extent, due to the fact that the advancement of technology has reshaped entirely our notion of privacy by extending its presence into digital spaces. As a result, neither privacy as a precondition for the exercise of other rights, nor privacy as a right by itself can be spoken about without taking into consideration the role that technologies play in our lives today.

As a response to 2013 Edward Snowden revelations about pervasive surveillance and increased awareness of data-gathering techniques used by tech-giants, privacy has become a major concern for civil society. Thanks to the efforts of digital rights advocates and technologists, encryption has become a widely used tool for protection of privacy online.

However, before becoming a widely available and user-friendly tool, cryptographic technologies were mainly under the control of the state bodies. As encryption started shifting into the public domain, the

[193] United Nations, General Assembly, Resolution adopted by the General Assembly on 18 December 2013, The right to privacy in the digital age, A/RES/68/167

governments faced a challenge – now anyone with access to software that helps encrypt emails or an end-to-end encrypted messenger could make their communications private.

Governments increasingly recognise the role and importance of cryptographic technologies in the digital age, especially in connection with the exercise of the rights to free speech, freedom of thought and opinion and the right to privacy. However, their response to the fact of wide accessibility of such technologies has been different. While some countries, like Germany, recognize the close interconnectedness of encryption with the exercise of individual rights to privacy and freedom of expression,[194] others attempt to restrict access to such technologies. The case studies of Turkey and Russia examined in this essay underscore the trend among non-democratic states to treat encryption as a tool that poses danger to national security and the status quo of the government. This is reflected full well in the amendments to the Russian Law on Information, Information Technologies and Protection of Information, which allow the Russian law enforcement to request encryption keys from the providers of electronic communication services without obtaining a judicial warrant. In Turkey, the coup attempt in July 2016 was followed by a large crackdown on the civil society, in which the fact of downloading an encrypted messaging app has become one of the main justifications for tens of thousands of arrests. To a different extent, the Russian legislation and the measures taken by the Turkish authorities during the state of emergency violated the countries' obligation under international human rights law.

[194] 'The international encryption debate: privacy versus big brother' (LEXOLOGY, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 3 September 2019

After an overview of the common themes present in the given case studies, the author makes several concrete recommendations that intend to directly address the challenges that have been posed to the integrity of encryption as a tool for protection of privacy and freedom of speech.

As such the author suggests that, taking into consideration its enabling and protective functions, encryption should receive a special consideration within the protection framework of international human rights law.

As exemplified by the case studies of Russia and Turkey, laws governing the use of technologies often have negative implications for the exercise of human rights. Taking this important factor into consideration, such laws should be shaped based on consultation with IT-experts, as well as national security and human rights experts, in order to ensure that legal requirements are realistic from technical standpoint, and that there is a balanced consideration of privacy and security arguments in the course of the law-making process.

Finally, the weakness of international framework for human rights protection necessitates special consideration for encryption as a tool for protection of the exercise of human rights online. If constitutional guarantees for the rights to freedom of speech and privacy can be easily bypassed by states invoking the notions of national security, then encryption, due to its protective and enabling functions, should be considered as a right which can be exercised by individuals as a measure to safeguard the rights and freedoms which are guaranteed to citizens.

This essay attempted to critically evaluate the existing legislation that governs the use of cryptographic technology in Russia and Turkey. The choice of the jurisdictions was made taking into consideration the negative effects that such laws have on human rights actors in the two countries. The analysis of the case-studies confirmed that the civil society activists, journalists and human rights defenders face prosecution under given laws, the ultimate aim of which is censorship of free speech, ideas and information sharing that is currently being protected by means of encrypted communication technologies.

This author of this essay does not aim at offering a solution to the challenges that the users of encrypted communication services face not only in non-democratic states, but also globally. Rather this essay is first step in developing a critical approach towards encryption and its role in the dominant narrative that is mostly shaped by juxtaposition of security and privacy arguments and the values associated with these notions. If there is one theme covered in this essay that the author finds hopeful is that there is a strong combination of values, rationales and arguments that emphasize the importance of encryption as something more than just a technical tool for privacy protection. Encryption is also a tool that gives individuals security and autonomy over their own privacy and communications – key aspects in the lives of individuals and in the work of human rights actors.

Bibliography

Academic articles (referenced and consulted)

1. Barendt, E. M. *Freedom of Speech.* Oxford University Press, 2007
2. Diggelmann, Oliver & Cleis, Maria Nicole. *How the Right to Privacy Became a Human Right.* Human Rights Law Review, Vol. 14, 2014, pp.441-458
3. Glancy J., Dorothy. *The Invention of the Right to Privacy.* Arizona Law Review, Vol. 21, 1979
4. Hankey, Stephanie & O Clunaigh, Daniel. *Rethinking Risk and Security of Human Rights Defenders in the Digital Age*. Journal of Human Rights Practice, Vol. 5, November 2013, pp.535-547.
5. Leith, Philip. *The Socio-legal context of privacy.* International Journal of Law in Context, 2,2 pp. 105-136 (2006)
6. Moor H, James. *Towards a Theory of Privacy in the Information Age.* Computer and Society, September 1997, pp. 27-32
7. Park, Susan. *The United Nations Human Rights Council's Resolution on Protection of Freedom of Expression on the Internet as a First Step in Protecting Human Rights Online.* North Carolina Journal of International Law and Commercial Regulation, Vol. 38, Issue 4 (Summer 2013), pp. 1129-1158
8. Plasencia, Adolfo & O'Reilly, Tim, 'Encryption as a human right', *Is the Universe a Hologram? Scientists Answer the Most Provocative Questions.* Cambridge: The MIT Press, 2017.
9. Sajo, Andras. *Freedom of Expression.* Institute of Public Affairs, 2004
10. Soldatov, Andrei & Borogan, Irina. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. Public Affairs, 2015.

11. Solove J. Daniel. *Conceptualizing Privacy*. California Law Review, Vol. 19, July 2002, pp. 1087-1155

12. Wachter, Sandra. *Privacy: Primus Inter Pares. Privacy as a precondition for self-development, personal fulfillment and the free enjoyment of fundamental human rights.* University of Oxford, October 2016

13. Warren D., Samuel & Brandeis D. Louis. *The Right to Privacy.* Harvard Law Review, Vol. 4, No 5, December 15, 1890, pp. 193-220

Reports and UN documents

1. Freedom on the Net 2017, Freedom House Report, 2017. Available at: https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf
2. Joint submission to the Universal Periodic Review of Turkey by Article 19, P24, PEN International, English PEN, Reporters Sans Frontiers (RSF), International Press Institute (IPI), Freemuse, European Centre for Press and Media Freedom (ECPMF), IFEX and Norsk PEN, July 2019.
3. Surveillance giants: how the business model of Facebook and Google threatens human rights, Amnesty International Report, 2019. Available at: https://www.amnesty.org/en/documents/pol30/1404/2019/en/
4. United Nations, Human Rights, Special Procedures, *Encryption and Anonymity follow-up report. Research Paper* 1/2018 available from https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

5. United Nations, General Assembly, Resolution adopted by the General Assembly on 18 December 2013, The right to privacy in the digital age, A/RES/68/167
6. United Nations, General Assembly, *Report of the Special Rapporteur on the Right to Privacy, A/71/368*
7. United Nations, Human Rights Committee, *General Comment No. 34*, CCPR/C/GC/34
8. United Nations, Human Rights Council, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/39/29 (3 August 2018)
9. United Nations, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27 (16 May 2011)
10. United Nations, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40 (17 April 2013)
11. United Nations, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression, David Kaye,* A/HRC/29/32 (22 May 2015)

Online Articles and Web pages

1. 'A Message to Our Customers' (Apple, 16 February 2016) <https://www.apple.com/customer-letter>
2. 'Another police informant emerges in a controversial case against an alleged Russian extremist group' (*Meduza*, 3 July 2018) <https://meduza.io/en/news/2018/08/27/another-police-informant-emerges-in-a-controversial-case-against-an-alleged-russian-extremist-group>

3. ‘Almost anyone can end up on the registry of Roskomnadzor’ (Tinkoff Journal, 8 February 2018)< https://journal.tinkoff.ru/news/ori/> (In Russian)
4. ‘Apple v. FBI’ (Electronic Privacy Information Center) <https://epic.org/amicus/crypto/apple/>
5. ‘Edward Snowden: ‘The people are still powerless, but now they’re aware’ (The Guardian, 4 June 2018) <https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware>
6. ‘Edward Snowden: the whistleblower behind the NSA surveillance revelations’ (The Guardian, 11 June 2013) <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>
7. ‘Encryption At The Centre Of Mass Arrests: One Year On From Turkey’s Failed Coup’ (Privacy International, 18 July 2017) <https://medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9>
8. ‘Freedom on the Net 2018, Report, Turkey’ (Freedom House) <https://freedomhouse.org/report/freedom-net/2018/turkey>
9. ‘Istanbul 10 Released’ (Front Line Defenders, 25 October 2017) <https://www.frontlinedefenders.org/en/case/istanbul-10-released-turkey>
10. ‘Podsadnye kukly’ (Novaya Gazeta, 27 August 2018) <https://novayagazeta.ru/articles/2018/08/26/77605-podsadnye-kukly> (in Russian)
11. ‘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>
12. ‘San Bernardino shooting: what we know so far’ (BBC, 11 December 2015)< https://www.bbc.com/news/world-us-canada-34993344>
13. ‘Secret Chats’ (Telegram) <https://telegram.org/faq#secret-chats>

14. ‘Taner Kilic Released’ (Front Line Defenders, 16 August 2018) <https://www.frontlinedefenders.org/en/case/istanbul-10-released-turkey#case-update-id-6815>
15. ‘Ten Human Rights Defenders Detained in Turkey’ (Front Line Defenders, 5 July 2017) < https://www.frontlinedefenders.org/en/profile/ten-human-rights-defenders-detained-turkey>
16. ‘Telecoms privacy and data security provisions in Turkey,’ Esin Attorney Partnership. (LEXOLOGY, 5 October, 2018)< https://www.lexology.com/library/detail.aspx?g=cfb4eba8-cc01-4b09-acf3-41a8c7b3d962>
17. ‘Telegram CEO Durov Says Russia's FSB Demands Messenger's Encryption Keys’ (RFE/RL, 27 September 2017)<https://www.rferl.org/a/telegram-durov-russia-fsb-encryption-keys-security/28760575.html>
18. ‘The Battle for Telegram moves to Strasbourg’ (Roskomsvoboda, 3 July 2019) <https://roskomsvoboda.org/47943/> (in Russian)
19. ‘The international encryption debate: privacy versus big brother’ (LEXOLOGY, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488>
20. ‘Turkey ends state of emergency after two years’ (BBC, 18 July 2018) <https://www.bbc.com/news/world-europe-44881328>
21. We need to talk about Turkey,’ (Amnesty International) https://www.amnesty.org/en/latest/campaigns/2018/04/turkey-human-rights-defenders-under-attack/

Laws and legal documents

1. Brief of Amici Curiae, Electronic Frontier Foundation and 46 technologists, researchers, and cryptographers, 22 March 2016, available at: https://www.eff.org/files/2016/03/03/16cm10sp_eff_apple_v_fbi_amicus_court_stamped.pdf
2. Communication by the Permanent Representative of Turkey to the Secretariat General of the Council of Europe, "Reservations and Declarations for Treaty No. 005 – Convention for the Protection of Human Rights and Fundamental Freedoms," 5 August 2016, Council of Europe, available at: https://www.coe.int/en/web/conventions
3. Constitution of the Republic of Turkey, available at: https://global.tbmm.gov.tr/docs/constitution_en.pdf
4. Constitution of the Russian Federation, available at: http://www.constitution.ru/index.htm
5. Decree of the Government of the Russian Federation of July 31, 2014 N 746
6. Electronic Communications Law of 2006, Turkey
7. Information note on the decree-law No. 699 of 31 July 2016 on the measures taken under the state of emergency, Turkey
8. Federal Law No. 149-FZ of July 27, 2006 on Information, Information Technologies and the Protection of Information, Russia
9. Federal Law on Counter-Terrorism (374-FZ), Russia
10. Information note on the decree-law No. 699 of 31 July 2016 on the measures taken under the state of emergency, Turkey