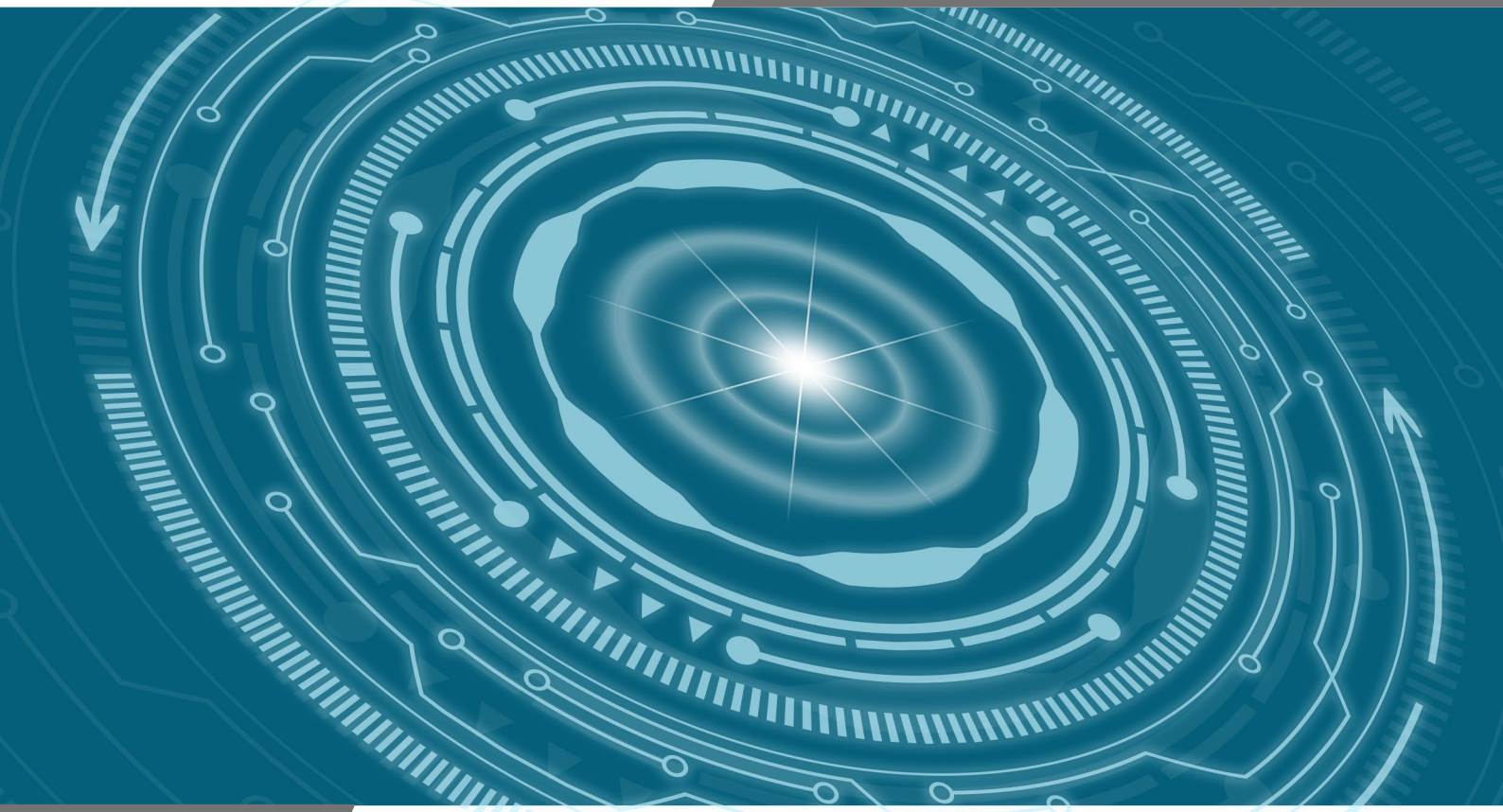
Centre for Economics and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2018/3



April 2018

Online freedoms and the European Court of Human Rights: a path forward for Turkey?

Yeşil Deniz | Research Assistant, EDAM

Online freedoms and the European Court of Human Rights: a path forward for Turkey?

Yeşil Deniz | Research Assistant, EDAM

Executive Summary:

The European Court of Human Rights is binding on the Turkish Constitutional Court since its ratification of the European Convention on Human Rights in 1954. Over the past 64 years, Turkey's track record against the European Court of Human Rights has proven that Turkey and the European human rights regime are increasingly plagued by structural differences. At the same time, Ankara remains reluctant to step down from its European membership bid. Turkey's convergence with the EU requires a fundamental change of understanding and practice. This paper marks an effort towards that end, with a focus on Internet rights and freedoms. It first lays down the European Convention on Human Rights' approach to privacy, freedom of expression and national security conflicts in cyberspace. The following section presents an analysis of three European Court of Human Rights cases to reveal the nature of the Court's assessment in balancing between Internet rights and freedoms and the competing interest of national security. The greater aim, which the concluding section seeks to address, is to offer how Turkey can bring its Internet Law in more conformity with the European human rights regime at a time when the freedom of expression online in particular finds itself so embattled in Turkey. This paper is a call for Turkey to periodically assess its level of respect and protection for the exercise of human rights and freedoms online from ethical, social and legal perspectives.

The research has been made possible by funding obtained from the US based Chrest Foundation

1. Introduction

Of the multiple international legal sources on human rights, none are more of an inspiration for Turkey than the European Convention on Human Rights (ECHR). The enforcement of the ECHR is provided by the European Court of Human Rights (ECtHR) set up in 1959. By ratifying the ECHR only 4 years after its signing in 1950 and accepting the obligatory jurisdiction of the ECtHR in 1990, Turkey promised to respect its obligations under the Convention and ensure full compliance with the case-law of the Court. The ratification of the Convention and subsequent accession to the Council of Europe demand the harmonization of national laws with the established standards of Europe. With the amendment to Article 90 of the Turkish constitution in 2004, international agreements were granted precedence over domestic laws in cases of conflict.[1] These expressed Turkey's then full commitment to Europe's legal sphere. Now, Ankara is still reluctant to step down from its membership bid. At the same time, in the words of the European Commission President Jean-Claude Juncker, it is moving away from Europe in "giant steps".[2]

In 2017, the ECtHR received 31,053 applications on Turkey. 30,063 were struck out or considered inadmissible. In 2017, the Court delivered 116 judgments, 99 of which found at least one violation of the European Convention on Human Rights. With this record, Turkey came second after Russia as the country with the most ECHR violations.[3] Among 116 judgments, 4 were found to violate Article 8 and 16 to violate Article 10 of the Convention, corresponding to 6% and 14% respectively.

Turkey's track record against the ECtHR between 1959 and 2017 is proof that Turkey and the European human rights regime are plagued by structural differences. With 3,385 judgments delivered and 2,988 found to be at least in one violation of the ECHR, Turkey ranked above all other Contracting State, surpassing Russia. Of these 104 corresponded to Article 8 (3%) and 281 to Article 10 of the Convention (9%).[4] As of 2018, 13.3% of applications are pending before the Court.[5]

To enhance Turkey's understanding of the European human rights regime on the Internet, this chapter builds on the ECHR's existing human rights standards and the ECtHR's enforcement mechanisms. It lays down the ECtHR's practice on privacy, freedom of expression and national security conflicts in cyberspace. The greater purpose is to highlight the importance of standard-setting within the context of the Internet and to explore how Turkey can bring its Internet-related standards more in conformity with the European regime. There lies the added value of this chapter: it offers best practice tools to foster the protection and exercise of fundamental freedoms and human rights on the Internet at a time when the freedom of expression online in particular finds itself so embattled in Turkey.

The core of provisions guaranteed by the ECHR for the right to respect for private and family life (Article 8) and the right to freedom of expression (Article 10) will be discussed. These are considered indicators that guide and enable Contracting States (States) in the proper exercise of individual rights and freedoms. The discussion on Articles 8 and 10 involves the description of the legitimate grounds that serve as a justification for the interference of a State against the implementation of a right or a freedom. This paper has a specific focus on national security, which is mentioned in paragraph 2 of Articles 8 and 10 as the first of the "legitimate aims" allowing legitimate restrictions. Yet, the Council of Europe's "National Security and European Case-Law" report acknowledges that the term national security is somewhat vaguely defined, affording it a degree of flexibility.[6]

While there is no doubt that the highly complex forms of espionage or terrorism necessitate States to take effective measures to preserve their national security, they are not

1 Arslan, Murat (2009): Comparing Constitutional Adjudication A Summer School on Comparative Interpretation of European Constitutional Jurisprudence, University of Trento, <http://www.jus.unitn.it/cocoa/papers/PAPERS%204TH%20PDF%5CJudges%20Turkey%20Arslan.pdf>

2 EURActiv (2017): "Juncker says Erdogan's Turkey is taking giant steps away from the EU", < https://www.euractiv.com/section/global-europe/news/juncker-says-erdogans-turkey-taking-giant-steps-away-from-eu/>

3 European Court of Human Rights (2017): Statistics, < https://www.echr.coe.int/Documents/Stats_violation_2017_ENG.pdf>

4 European Court of Human Rights (1959-2017): Statistics, < https://www.echr.coe.int/Documents/Stats_violation_1959_2017_ENG.pdf>

5 European Court of Human Rights (2018): Statistics, < https://www.echr.coe.int/Documents/Stats_pending_2018_BIL.pdf>

6 European Court of Human Rights Research Division (2013): National Security and European case-law, <https://rm.coe.int/168067d214>

permitted (under the jurisdiction of the ECHR) to exercise unlimited discretion in the name of this battle. Balancing between the right and freedom at hand and national security considerations involves a prime legal decision-making process, which the ECHR dubs the "three-part-test". This test, uniformly applied by the ECtHR, ensures that States do not abuse their power by disproportionately or arbitrarily forfeiting the rights guaranteed by the Convention, for example through excessive online censorship or surveillance for the protection of national security. If a State ignores the ruling of the Court, the provisions of the Convention are directly or indirectly binding, i.e. the Court may impose fines, or the State may risk its international standing due to the verdict of the Court. The judgments of the Court are declaratory in nature: the ECtHR's decision against any other State serves as a reference to which Turkey must equally adhere to, thereby protecting itself against possible findings of violations.

This discussion is followed by an analysis of three ECtHR cases. The aim of this task is not to provide an exhaustive list of all relevant decisions handed out by the Court. Rather, the objective is to reveal the nature of the ECtHR's assessment – elucidating the questions raised and issued prioritized – in balancing between the rights enshrined in Articles 8 and 10 and the legitimate aim of national security within the context of the Internet. The concluding section presents recommendations to align Turkey's Internet Law (Law No. 5651) in more conformity with the European human rights standards.

2. The ECHR as a "living document" and its people-centered human rights approach to the Internet

Since its signing in 1950, the Convention progressed and broadened in scope by the works of the ECtHR, the European Commission of Human Rights and the Council of Europe.[7] Referred to as a *living document*,[8] the Convention continuously broadens the rights afforded, and applies them to circumstances that were not previously conceivable. In its "Guide to Human Rights for Internet Users" prepared based on the ECHR and its interpretation by the ECtHR, the Council of Europe stated; fundamental freedoms and human rights apply equally online and offline.[9] By way of this statement, the Council of Europe obliged States like Turkey to secure the respect for rights and freedoms in the context of the Internet by ensuring no Internet user is subject to illegitimate, unnecessary or disproportionate interference with the implementation of their rights and freedoms.[10] In fact, freedom of expression was recognized as a core value of the Internet in *Yıldırım v.* Turkey in the following terms:

> *"The Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest."*[11]

Delfi AS v. Estonia is another widely cited case to demonstrate the Convention's uniform approach to offline and online, subjecting the Internet to "tangible" principles. This case ratified the non-discriminatory application of Article 10 of the Convention to the Internet, despite the nature of the message and even when exercised for commercial speech.[12] It was also with this case that the Court recognized the risk of violating Article 8 of the Convention was higher on the web compared to printed press, while equally acknowledging its potential to extend the freedoms of speech and expression.[13] Thus, it was a question of weighing two competing interests, equally protected by the ECHR.

Acknowledging the influence of modern technologies, the Court expanded the scope of Article 8 to include e-mail

7 Macovei, Monica (2004): A guide to the implementation of Article 10 of the European Convention on Human Rights, <https://rm.coe.int/168007ff48>

8 European Court of Human Rights (n.d.): The ECHR in 50 questions, <http://www.echr.coe.int/Documents/50Questions_ENG.pdf>

9 Council of Europe (2014): Guide to Human Rights for Internet Users, <https://rm.coe.int/16804d5b31>

10 ibid.

11 European Court on Human Rights, Yildirim v. Turkey, No. 3111/10, [54]

12 European Court on Human Rights (2015): Internet: case-law of the European Court of Human Rights, <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf>, p. 17

13 European Court on Human Rights, Delfi AS v. Estonia, No. 64569/09, [133]

communications in *Weber and Saravia v Germany*.[14] Access to the Internet was ratified in *Kalda v. Estonia* as a right for all. The Internet's public-service value was recognized in countless cases. Measures to promote this public-service value were adopted by the Committee of Ministers in 2007.[15] These are exemplary of the ECHR's interpretive technique and contemporary approach to legal decision-making as enforced by the ECtHR.

Under the Convention, national courts hold the first and foremost position to ensure the free exercise of individual rights and freedoms. Any application to the Court must only be after all domestic remedies are exhausted – meaning, the Court must only be the last resort. Therefore, the primary objective of the ECHR is the guarantee of individual rights and freedoms through the enforcement of States via their respective governments and courts. Since almost all Contracting States have integrated the provisions of the Convention into their national legislations, it follows that national judges accommodate to the Court's jurisprudence as a standard-setter. This prioritization of States in the sequence of the Convention's decision-making process endows States, like Turkey, with the obligation to ensure their national legal systems do not run afoul of the evolving values of the ECHR. The extent to which Turkey follows suit, while accommodating for deeper structural differences will undoubtedly define how well it interacts with the European human rights regime. The primary challenge for Turkey is to remain aware of and receptive to the ECHR's evolving standards, including its regulations in cyberspace.

What is equally revealing about the European approach is its vision to inform and empower Internet users of their rights and freedoms as a principle of Internet governance. This approach was affirmed by the Committee of Ministers in its "Declaration on Internet Governance Principles" of 2011, as a people-based and human rights perspective to the Internet.[16] Efforts towards cultivating a similar understanding of Internet governance would bring Turkey's standards closer to those of Europe.

Turkey should work to inform Internet users of the different choices they make online and the costs of giving consent to such decisions. It should ensure that Internet users are aware of the limitations of their rights and the redress mechanisms available. More so, it should periodically assess its level of respect and protection for the exercise of human rights and freedoms online from ethical, social and legal perspectives, including evaluations on governance accountability and transparency mechanisms.

3. Article 8 of the ECHR: Respect for private and family life

The rapid expansion of the Internet and the advent of similar technologies have revolutionized the way individuals communicate. Where Internet technology is routed allows governments to track communications, subject them to detailed and sometimes intrusive profiling and analyze individuals' private lives. Items purchased, websites visited, forums joined, movies watched, or books read are all pieces of communications data that deliver a great wealth of detail about an individual's private life. Though surveillance practices by means of scooping communications data may also be closely linked to the right to freedom of expression (if, for instance, state powers are used to circumvent the protection of a journalistic source), they are usually assessed against Article 8 alone.

Article 8 of the ECHR protects the right to respect for private and family life in the following terms:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*[17]

[14] European Court on Human Rights, Weber and Saravia v Germany, No. 54934/00, [77]

[15] Council of Europe, Committee of Ministers (2016): Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d4a39>

[16] Council of Europe, Committee of Ministers (2011): Declaration by the Committee of Ministers on Internet governance principles, adopted on 21 September 2011, <https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl%2821.09.2011_2%29&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864-%20EN&direct=true>

[17] European Court on Human Rights (2016): Guide on Article 8 of the European Convention on Human Rights, <http://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>

While paragraph 1 (Article 8 §1) lays down the rights that a Contracting State must guarantee to individuals, paragraph 2 (Article 8 paragraph 2 (§2), verifies that the rights provided in Article 8 §1 are not absolute. This is a fundamental takeaway for Turkey: The State may legitimately restrict the enjoyment of the respect for private and family life, however, only under certain circumstances subject to strict interpretation.

For Article 8 to apply, the Court firstly assesses whether the right, which an individual invokes has been restricted, is guaranteed by Article 8 §1 –i.e. Article 8 only applies to those cases that involve at least one of the four interests: private life, family life, home and correspondence. The protection and retention of personal data, such as home address, always falls within the scope of Article 8 of the Convention.[18] This assessment of applicability entails a discussion of what constitutes private life or home within the meaning of Article 8. As expressed in many cases (see for example *E.B. v. France; Niemietz v. Germany; Pretty v. the United Kingdom*; Peck v. the United Kingdom), these terms cannot be exhaustively defined. In return, such lack of strict definition allows the Court's case-law to evolve in consideration of technological and other social developments, reinforcing its interpretive technique.

If the Court determines that the right concerned does not fall within the scope of Article 8 §1, the complaint will end there. If, on the other hand, Article 8 applies, the Court will consider whether the interference can be justified by the circumstances set out in Article 8 §2. Since the interception of online communications data bears a high potential for unwarranted intrusion, the purposes for which States' interception with privacy may be permitted are strictly enumerated. Accordingly, a State may legitimately interfere with privacy through, for example, collecting and storing personal information online, if it is in the interest of national security. In fact, in *Kopp v. Switzerland*, the Court noted, "[…] when national security is at stake […] there are no conversations for which surveillance should be prohibited".[19]

In cases involving suspected terrorists, States enjoy a wider "margin of appreciation",[20] especially with regards to the storage of information of individuals implicated in past terrorist activities.[21] This differentiation is telling of the Court's legal decision-making process: The Court considers the specific context in which personal data is obtained and stored as well as the nature of the information concerned.

At the same time, the Court requires any monitoring of this kind to be adequately supervised. An Internet user must know what personal data are processed or transferred to third parties, when, by whom and for what reason.[22] With respect to secret surveillance, a State must also provide legal guarantees that concern the supervision of related services. These may include the scope, nature and duration of possible measures, the reasons required for instructing them, the competent authorities to approve, executive and oversee such measures and the remedies provided under national law or any other related condition. Otherwise, the State's execution of secret surveillance could destabilize the functioning of democracy on the contrary ground of maintaining it. What this means for Turkey is straightforward: the effective operation of privacy is a defining quality of democracy, the lack of which should be handled with the utmost possible skepticism.

Where the case concerns a restriction to the exercise of Article 8, the Court will decide whether the interference was "in accordance with the law", "pursued a legitimate aim" and was "necessary in a democratic society". This three-part approach is discussed in more detail below. The application lodged before the Court does not exclusively need to entail an interference by a State. Applicants can also complain that the State or other public authorities should have, albeit failed to, take action, which the applicant deems necessary to guarantee his or her rights enshrined in Article 8. Thus, a State may be held liable for its acts (negative obligations) as well as omissions (positive obligations).

---

18 European Court on Human Rights (2015): Internet: case-law of the European Court of Human Rights, <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> and Kilkelly, Ursula (2003): A guide to the implementation of Article 8 of the European Convention on Human Rights, <https://rm.coe.int/168007ff47>

19 in European Court of Human Rights Research Division (2013): National Security and European case-law, <https://rm.coe.int/168067d214>, p. 9

20 This doctrine refers to the room for maneuver (i.e. the degree of latitude) national authorities are provided with to meet their obligations under the Convention considering their own legal and cultural traditions.

21 European Court on Human Rights, Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, [88]

22 Council of Europe (2014): Guide to Human Rights for Internet Users, <https://rm.coe.int/16804d5b31>

4. Article 10 of the ECHR: Freedom of expression

The right to inform the public and the public's right to receive information are not absolute and may be sacrificed if countervailing public interests are at risk. Public order and national security are recognized by the Court as legitimate grounds for restricting freedom of expression online, because it is considered that a State under threat cannot guarantee any rights and freedoms to its citizens. However, as measures carried in the name of national security may be instrumentalized by States for political grounds, the Court calls for a fair balance between different interests at stake. Such tension between freedom of expression and national security has given rise to a substantial number of cases, including from Turkey. "The Court has had to deal with a number of Turkish cases [on Article 10 against] the Law on the prevention of terrorism, particularly the prohibition of propaganda destined to undermine the territorial integrity of the state".[23] The number of cases lodged before the Court is symptomatic of the effectiveness of a State's domestic remedies.

Article 10 of the Convention stipulates:

> *"1. 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. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> *2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions, or penalties as are prescribed by law and are necessary in a democratic society, in the interest of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."*[24]

The first paragraph (Article 10 §1) points to the following elements of the right to freedom of expression online, which must be exercised freely and without interference by public authorities:

- *Freedom to hold opinions,*
- *Freedom to receive information and ideas, and,*
- *Freedom to impart information and ideas.*

As individual opinions cannot be entirely known – hence, regulated – the freedom to hold opinions online enjoys an almost absolute protection under Article 10. According to the Committee of Ministers, "any restrictions to this right will be inconsistent with the nature of a democratic society".[25] Restrictions to this right include any attempt by the State to indoctrinate its citizens or discriminate against certain individuals based on their opinions.

Of special importance is the acknowledgement that a State's promotion of biased information engenders a serious barrier to the freedom to hold opinions. The freedom to hold opinions online equally protects the reverse freedom of non-disclosure: An Internet user may choose not to share his/her opinions online.[26] As a member of Council of Europe striving to join the EU bloc, Turkey is expected to abide by the same rules.

Users have the right to receive and impart information on the Internet, particularly to create, re-create and distribute content on the web. The freedom to impart information and ideas is not only applicable to information and ideas that are positively admitted or deemed harmless, but also to those that "offend, shock or disturb … [for] such are the demands of pluralism, tolerance and broad-mindedness without which there is no democratic society".[27] Broadly speaking, the freedom to impart information and ideas online provides Internet users the right to tell others what s/he thinks or knows in public or in private. This guarantee permits the free criticism of the government, seen as an indispensable component of democracy. For the Court,

[23] European Court of Human Rights Research Division (2013): National Security and European case-law, <https://rm.coe.int/168067d214>, p. 19

[24] European Convention on Human Rights (n.d.), <http://www.echr.coe.int/Documents/Convention_ENG.pdf>

[25] Dijk et al. (2006): Theory and Practice of the European Convention on Human Rights, p. 413

[26] Vogt v. Germany in Macovei, Monica (2004): A guide to the implementation of Article 10 of the European Convention on Human Rights, <https://rm.coe.int/168007ff48>

[27] Handyside v. the United Kingdom in Mendel, Toby (n.d.): A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights, <https://rm.coe.int/16806f5bb3>, p. 5

even seemingly flawless elections cannot be regarded meaningful if citizens are not allowed to fully express themselves. Drawing a clear line between information (facts) and opinions (value judgments), the Court stated the following:

> *"The existence of facts can be demonstrated, whereas the truth of value judgments is not susceptible to proof […] as regards value judgments this requirement is impossible of fulfilment and it infringes freedom of opinion itself, which is a fundamental part of the right secured by Article 10 of the Convention".*[28]

Accordingly, Article 10 protects opinions, critiques or speculations that cannot be subjected to truth proof, just as it protects information that can be verified. There lies the ethos of the ECHR: value judgments, particularly on politics, enjoy special protection, as they constitute the cornerstone of a democratic society. Complementary to the freedom to impart information and ideas, Article 10 provides the right to gather and seek information and ideas through all possible legitimate sources. The right of the public to be adequately informed, particularly on matters of public interest is guaranteed in the exercise of this freedom. These two rights are not absolute and must be weighed against the rights of Internet users and the needs of a democratic society. Since hate speech falls against the needs of a democratic society, it is under no condition protected by Article 10 of the ECHR.[29]

Akin to the structure of Article 8, Article 10 §2 infers that the right to freedom of expression online is not unconditional. Yet, these circumstances must be known to the Internet user, along with information on ways to seek guidance and redress, and not be broader or sustained for longer than is strictly necessary to achieve its purpose.[30] In fact, the Court repeatedly indicated that Article 10 §2 leaves little room for restrictions in matters of public interest. In legal terms, comments that contribute to public interest generally enjoy a high-level of protection of freedom of expression, which means that the margin of appreciation left to State authorities is particularly narrow.[31] Yet, the Internet is equally subject to scrutiny and protection as regards respect for free contribution to political debate. Even in the context of a debate on public interest, any damage suffered by public authorities or private individuals as a result of disclosure should not compromise incitement to hatred or violence (see for example, *Sürek and Özdemir v. Turkey*[32]). An individual is allowed a degree of exaggeration or even provocation to make somewhat immoderate statements on public matters, insofar as he or she does not overstep certain limits, i.e. respect for the rights of others.[33]

Inspired by the Convention's Implementation Guide, which is published by the Council of Europe,[34] the following section extrapolates certain phrases within Article 10 §2. Although the Guide disclaims that the opinions expressed are those of the author and not of the Council of Europe, it nonetheless unlocks the kind of factors that the Court considers in its decision-making process.

> *"The exercise of these freedoms […] may be subject to […]"*

The Guide specifies that under Article 10 §2, national authorities have only the option and not the obligation (*"may be subject to"*) to impose a restrictive measure to the exercise of the right to the freedom of expression online.

> *"The exercise of these freedoms, since it carries with it duties and responsibilities […]"*

This phrase is unique to the Convention. For the press, which enjoys a significant presence on the Internet, freedom to impart and receive information, and the guarantees afforded to it are of particular importance, because the press has a duty to impart information and ideas on matters of public interest.[35] The right of the public to receive information depends on the ability of the press to freely exercise their job (see for example *Observer and*

---

[28] see for example European Court of Human Rights, Lingens v. Austria, No. 9815/82

[29] Council of Europe (2014): Guide to Human Rights for Internet Users, <https://rm.coe.int/16804d5b31>

[30] ibid.

[31] see for example European Court of Human Rights, Axel Springer AG v. Germany, No. 39954/08, [90]

[32] in European Court of Human Rights Research Division (2013): National Security and European case-law, <https://rm.coe.int/168067d214>, p. 17

[33] see for example European Court of Human Rights, Willem v. France, No. 10883/05, [33]

[34] Macovei, Monica (2004): A guide to the implementation of Article 10 of the European Convention on Human Rights, <https://rm.coe.int/168007ff48>

[35] see for example European Court of Human Rights, Observer and Guardian v. the United Kingdom, No.13585/88

Guardian v. the United Kingdom[36]). Therefore, by no means should the sanction imposed on a journalist disclosing confidential information limit access to information that the public is entitled to receive and must therefore be justified by particularly compelling reasons.[37] The measure enacted should not amount to a form of censorship intended to discourage the press from voicing criticism or performing its task as purveyor of information and public watchdog.

Turkey's state of press freedom stains its image in the eyes of Europe. In 2017, the ECtHR stated it will prioritize applications regarding press freedom and journalists, an amendment most likely triggered by Turkey, Russia and Azerbaijan.[38] Turkey ranked the 155th out of 180 countries in the 2017 Press Freedom Index, four points lower than the year before.[39] The imprisonment of Deniz Yücel, a German-Turkish journalist who was detained for more than a year, was a serious irritant in German-Turkish ties.[40] Currently, Turkey is the world's worst jailer for journalists with a record of 73 journalists behind bars in 2017.[41] Turkey lacks a common ground with the ECHR on the definition and implementation of the freedom of press.

> *"The exercise of these freedoms […] may be subject to formalities, conditions, restrictions or penalties […]"*

According to the Guide, this phrase infers that the range of interference with the exercise of freedom of expression online is wide-ranging, including criminal convictions, obligations to pay civil damages, sentencing, prohibition of publications, or the ban of the exercise of the profession.[42] Of the many interferences, the Court deems criminal conviction and sentencing as the most threatening for the exercise of the freedom of expression online. The Court argues that criminal penalties, even in relatively insignificant amounts, may induce censorship, curbing public discussion.

> *"[…] in the context of the political debate such a sentence would be likely to deter journalists from contributing to public discussion of issues affecting the life of the community. By the same token, a sanction such as this is liable to hamper the press in performing its tasks as purveyor of information and public watchdog".*[43]

Although Article 10 does not explicitly refer to the press in writing, the extensive set of principles and rules developed by the Court grants the press a privileged position in the enjoyment of the freedoms protected under Article 10. The status of the press as a "political watchdog" was first ratified in the Lingens v. Austria case,[44] where national courts' imposition of a fine against a journalist for alleged defamatory statements was dismissed by the Court: opinions cannot be subject to being proven.

Even with regards to information, the Court acknowledged the "defense of good faith" as affording the press "a breathing space for error".[45] In *Dalban v. Romania* the Court stipulated, "there is no proof that the description of events given in the articles was totally untrue and was designed to fuel a defamation campaign."[46] This judgment proves that in cases where a publication holds a legitimate purpose, the issue is of public concern, and appropriate measures have been taken to validate the facts; the press cannot be legally responsible, even if the aforementioned facts are proven untrue.

---

36 ibid.

37 see for example European Court on Human Rights, Timpul Info-Magazin and Anghel v. Moldova, No. 42864/05

38 Hurriyet Daily News (2017): Euro court to prioritize applications regarding press freedom, journalists, <http://www.hurriyetdailynews.com/euro-court-to-prioritize-applications-regarding-press-freedom-journalists-113792>

39 Reporters Without Borders (n.d.): Journalism engulfed by the purge, <https://rsf.org/en/turkey>

40 BBC News (2017): German Die Welt reporter Deniz Yucel to leave Turkey jail, <http://www.bbc.com/news/world-europe-43083469>

41 Hurriyet Daily News (2017): Turkey worst in world for jailed journalists for second year: CPJ report, <http://www.hurriyetdailynews.com/turkey-worst-in-world-for-jailed-journalists-for-second-year-cpj-report-124100>

42 ibid, p. 25

43 see for example European Court on Human Rights, Lingens v. Austria, No. 9815/82

44 ibid.

45 ibid.

46 see for example European Court on Human Rights, Dalban v. Romania, No. 28114/95

5. The three-part test: the standard assessment of the ECtHR

As enumerated in Article 8 §2 and Article 10 §2, national authorities may legitimately interfere with the exercise of these rights and freedoms. However, such interference can only be legitimate if the following conditions are met in the order of appearance:

- *"The interference (meaning "formality", "condition", "restriction" or "penalty") is prescribed by law;*
- *The interference is aimed at protecting one or more of the following interests or values: national security; territorial integrity; public safety; prevention of disorder or crime; protection of health; morals; reputation or rights of others; preventing the disclosure of information received in confidence, and; maintaining the authority and impartiality of the judiciary;*
- *The interference is necessary in a democratic society".*[47]

5.1. Legality

Legality stands as one of the key principles of the Court's three-part test, which dictates that any injunction to the right to respect for privacy and family life or the freedom of expression to be legitimate must be solidly grounded in law. This equally holds that the impugned measure must be foreseeable, clear and adequately accessible to the subject involved, who must then be able to reasonably assess the consequences of his/her choices.[48] For instance, the Court found a violation of Article 8 in *Vukota-Bojić v. Switzerland*[49] because national legal provisions, which had served as the legal ground for the applicant's surveillance, lacked clarity and precision. Where secret surveillance is exercised in the interest of national security, the criteria of "foreseeability" cannot require individuals to predict what sort of controls the police may execute. Rather, the Court argued in *Leander v. Sweden*; it suffices for national law to clearly provide individuals with an adequate indication on the conditions that will allow public authorities to resort to secret surveillance.[50] This exemplifies the Court's case-by-case approach.

If the Court finds that the interference in question was not enshrined in national law, the responsible State would expressly be found in violation. The Court would not need to further assess whether the interference pursued a "legitimate aim" or was "necessary in a democratic society".[51] The sequence of the criteria, with national law requirements as the first pre-requisite of legitimate interference, is proof that the Court prioritizes the qualified enforcement of States' legal systems. This should reassure Turkey and Contracting States alike that it is in their will to "get along" with the ECtHR.

5.2. Legitimacy

If the restriction passes the first criteria, the Court will then assess whether it pursued a legitimate aim. To recap, for an interference to be deemed legitimate by the Court, the State cannot invoke just any aim. In fact, the second paragraph of Articles 8 and 10 strictly interpret the legitimate aims in pursuit of which those rights and freedoms may be restricted. For example, since national security is not listed as a legitimate aim in Article 9 of the Convention (the right to freedom of thought conscience and religion), any State interference on the grounds of national security would be a clear violation of that right. Regarding interferences to protect a State's national security, the Court generally accepts the legitimacy of the aim sought, affording the State a wide margin of appreciation. In fact, in *Kopp v. Switzerland* the Court held that there are no conversations for which surveillance should be prohibited if national security is at stake.[52]

5.3. Necessity

The Court's tendency to accept the state's appraisal of national security justifications, places the focus on the necessity criteria. This amounts to the most open-ended and complex stage of its three-part test. To begin with, the characteristics that make up a democratic society have

[47] Macovei, Monica (2004): A guide to the implementation of Article 10 of the European Convention on Human Rights, <https://rm.coe.int/168007ff48>, p. 29

[48] see for example European Court on Human Rights, Ekin v. France, No. 39288/98

[49] European Court of Human Rights, Vukota-Bojić v. Switzerland, No. 61838/10

[50] European Court of Human Rights Research Division (2013): National Security and European case-law, <https://rm.coe.int/168067d214>, p. 8

[51] European Court of Human Rights, M.M. v. the Netherlands, No. 39339/98, [46]

[52] in European Court of Human Rights Research Division (2013): National Security and European case-law, <https://rm.coe.int/168067d214>

not been specified in detail. However, there are several pointers; in *Dudgeon v. the United Kingdom*,[53] the Court referred to broadmindedness and tolerance as two pillars of a "democratic" society.

Although not expressly mentioned in Article 8 §2 and Article 10 §2, the condition of necessity itself implicates several elements: the measure must serve a pressing social need; it must be proportionate to the legitimate aim pursued;[54] and the Court must certify that the reasons provided by the State are relevant and sufficient.[55] The principle of proportionality requires the interference to be the least intrusive means available. In *Uzun v. Germany*, the Court noted that GPS surveillance interfered less with a person's private life in comparison to other methods of visual or acoustic surveillance,[56] whereas, secret surveillance is tolerable only if it is strictly necessary for protecting democratic institutions.[57]

It appears that the Court discards excessively strict or absolute interpretations of necessity, rather recognizing that the exercise of an individual's rights must always be weighed against the broader public interest.[58] In principle, the condition of necessity in a democratic society for the purposes of Article 8 and Article 10 is determined by balancing individual rights and the public interest of States. Assessing whether an interference was necessary, the Court also considers the margin of appreciation left to State authorities. This principle infers that what can be restricted may vary from one country to another. However, it would be left to Turkey to demonstrate the existence of the pressing social need behind the interference.[59]

Pursuant to necessity, the Court held in multiple cases that owing to the Internet's capacity to copy, mirror and disseminate information, restricting publications on certain content that is otherwise available was not necessary in a democratic society.[60] According to the Center for Democracy and Technology:

> *"The necessity principle may also be relevant to the Internet in contexts where the availability of user controls makes government control unnecessary […] Because the Internet is an interactive medium, citizens have far more control over what information reaches (or does not reach) their computer screens than with traditional forms of broadcast media".*[61]

While national authorities are responsible for the initial assessment of the restriction, the final evaluation remains subject to review by the Court. If the Court decides that all three conditions are met, the interference by the State will be regarded as legitimate, albeit the burden to verify that all three conditions are fulfilled remains with the State. If, however, the Court finds that the State fails to prove these conditions, it will concur that the interference was illegitimate without any further examination, i.e. the rights and freedoms have expressly been violated.

The main challenge with this criterion is the principle of margin of appreciation afforded to Contracting States. Turkey's continued disbelief in the European member states' understanding of the real threat posed by the failed coup attempt in July 2016 confirms that any doubt on the sincerity of European institutions may weaken a State's impetus for compliance and further legislative reforms. Any assessment by the ECtHR should also account for the existence of trust between a State and the greater European framework, or its lack of.

---

53 European Court of Human Rights, Dudgeon v. the United Kingdom, No. 7525/76, [53]

54 Centre for Democracy and Technology (2011): "Regardless of Frontiers": The International Freedom of Expression in the Digital Age Discussion Draft, <https://cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf>

55 see for example European Court of Human Rights, Bladet Tromsø and Stensaas v. Norway, No. 21980/93

56 European Court of Human Rights, Uzun v. Germany, No. 35623/05

57 European Court of Human Rights, Kennedy v. United Kingdom, No. 26839/05

58 Kilkelly, Ursula (2003): A guide to the implementation of Article 8 of the European Convention on Human Rights, <https://rm.coe.int/168007ff47>

59 see for example European Court of Human Rights, Piechowicz v. Poland, No.20071/07 [212]

60 see for example European Court of Human Rights, Observer and Guardian v. the United Kingdom, No.13585/88

61 Centre for Democracy and Technology (2011): "Regardless of Frontiers": The International Freedom of Expression in the Digital Age Discussion Draft, <https://cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf>, p. 25

6. The analysis of the ECtHR's case-law through three prominent cases

Up till now, this chapter laid down the right to respect for private and family life as protected under Article 8 §1 and the freedom of expression protected in Article 10 §1 as fundamental, albeit not absolute rights to the functioning of a democratic society in the interest of national security. It recognized that States have a certain measure of discretion when evaluating threats to national security and when deciding how to combat these, including interfering with the exercise of rights and freedoms, provided it is justified by law, proportionate to the legitimate aim pursued, and necessary in a democratic society.

The following discussion analyzes the Court's case-law on specific issues raised within the context of the Internet to demonstrate its practical approach to the meanings of the rights and freedoms enshrined in Article 8 §1 and Article 10 §1, and national security as one of the legitimate interests provided in the second paragraphs of the same articles. It equally seeks to assign some substance to the concept of national security, otherwise defined in somewhat vague terms.

6.1. Mass surveillance: 10 Human Rights Organisations and Others v. the United Kingdom

A very relevant development for this research occurred on November 7, 2017, when the Court held a Chamber hearing for the case of *10 Human Rights Organisations and Others v. the United Kingdom*,[62] brought by ten human rights organizations that have contact with non-governmental organizations, journalists, politicians, lawyers, whistle-blowers and more under, inter alia, Article 8 of the Convention. The mode of their communications is reported to vary with each audience, including e-mails, social media as well as instant messaging. The applicants report that the information they hold often includes sensitive, classified and to a certain extent, privileged content. For this reason, the applicants argue that the United Kingdom intelligence services may have intercepted the content of their confidential communications and their communications data, pursuant to the Regulation of Investigatory Powers Act (2000), under the domestic interception programme, Tempora, or through Prism or Upstream programmes, operated by the United Sates National Security Agency (NSA). As reported by the applicants, the United States has had access to the data collected by Tempora. The case invites the Court to assert how human rights standards accommodate to current state surveillance capabilities in the age of digital communication. "The case challenges the U.K. government's bulk interception of Internet traffic transiting through undersea fiber optic cables landing in the U.K., as well as its access to communications and data intercepted in bulk by the intelligence services of other countries, such as the NSA".[63] The case also seeks to unravel the confidential resource-sharing agreements of the United Kingdom and the United States, allowing the data as well as the intelligence collected abroad to travel between those two countries.

What renders the *10 Human Rights Organisations and Others v. the UK* case interesting, beyond its application of digital communication within the jurisdiction of Article 8 of the Convention, is that it is the first case to appear before the Court to directly challenge "mass surveillance" as revealed by Edward Snowden, a former systems administrator with the NSA. In 2013, Snowden leaked information disclosing the NSA's mass surveillance programmes. According to the information provided, the NSA's Prism programme enables access to the content of communications, including personal e-mails, chats, documents or links, and communications data, which reveals the identity and location of Internet users. The leaked documents verify that the Prism was used by the United Kingdom Government Communications Headquarters (GCHQ) to produce intelligence reports, confirming that the United Kingdom has had access to hundreds of millions of data and metadata intercepted by the NSA. Snowden disclosures also showed that content and communications data from fiber-optic cables and infrastructure maintained by U.S. communications service providers is collected through the NSA's Upstream programme, with access to global data, particularly of non-US citizens. GCHQ's own

[62] European Court of Human Rights, 10 Human Rights Organisations and Others v. the UK, No. 24960/15

[63] Callander, Ailidh and Kim, Scarlet (2017): European Court Ruling Could Recognize Mass Surveillance Violates Human Rights, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/european-court-ruling-could-recognize-mass>

surveillance programme, Tempora, which bears similarities to the Upstream programme, probes content and communications information passing through fiber-optic cables running from the United Kingdom to North America. These probes allow intelligence agencies to extract Internet traffic and filter it according to "search criteria". However, the full scope of permissible search criteria or the existence of any meaningful regulation or oversight of their use remains unknown.

Although the ruling of the Court will be made at a later stage using its three-part analysis and based on the exigencies of the situation, earlier discussions on the approach of the Court may be indicative of its possible decision. The nature of mass surveillance allows States to collect all communications all the time indiscriminately, therefore ruling out targeting and the requirement of reasonable suspicion. This naturally threatens the right to privacy, as the very essence of the privacy of communications is that interferences must be exceptional and justified on a case-by-case basis. The nature of mass surveillance would potentially jeopardize the principle of proportionality, which requires the government to disprove the existence of a less intrusive measure when entrenching on fundamental rights and freedoms.

Additionally, the Court is likely to take into consideration the decisions of independent European advisory bodies as guidance. In 2014, the independent European advisory body of EU Data Protection Working Party, established under Article 29 of the EU Directive 95/46/EC published its opinion on the surveillance of electronic communications for the purposes of intelligence and national security. Accordingly,

> *"[…] secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society".*[64]

In line with the opinion of the EU Data Protection Working Body, and its consideration of proportionality, it would appear that the Court is categorially against mass surveillance within the context of the Internet.

Yet, the *Szabó and Vissy v. Hungary* case provides an alternative reading, a drift from the assumption that mass surveillance programmes are inherently against the mandate of the ECHR. In the case, the Court stated that mass surveillance programmes are in fact inevitable in the face of vast technological changes and capabilities. This was also the starting point of the Venice Commission in its 2015 Report on Democratic Oversight of Signals Intelligence Agencies. In particular, the Court found in *Szabó* and *Vissy v. Hungary* that:

> *"[…] it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents."*[65]

The Court therefore did not question whether the "blanket" power of mass surveillance programmes was inherently incompatible with the requirements of the Convention. Rather, the Court proceeded with the assessment of whether sufficient safeguards existed and held, there had been violation of Article 8 of the ECHR as the legislation in question lacked sufficient guarantees against abuse. The Court further considered that a central issue in the case was the absence of judicial supervision. The Court concluded that in the field of secret surveillance, control by an independent body - normally a judge with special expertise - should be the rule and not the exception.

For Article 19, an NGO operating in the United Kingdom, the Court's recognition of NGOs as public watchdogs equivalent to that of the press in previous cases (see *Társaság a Szabadságjogokért v Hungary*) should afford the applicants in *10 Human Rights Organisations and Others v. the UK* the same legal protections as the press, including the protection of journalistic source and confidentiality of communications.[66] Following its previous verdicts, the Court may indeed argue that the interception powers and capabilities of intelligence agencies to capture NGOs' online communications have a chilling effect on

[64] Article 29 of Directive 95/46/EC, <http://www.ohchr.org/Documents/Issues/Privacy/ECArticle29DataProtectionWorkingGroup.pdf>

[65] European Court of Human Rights, Szabó and Vissy v. Hungary, No. 37138/14

[66] Article 19 (n.d.): Third Party Intervention Submission, <https://www.article19.org/data/files/medialibrary/38293/10-HRO-v-the-UK-A19-submissions-March-2016.pdf>

NGOs public watchdog function by eroding the willingness of people to communicate sensitive information, detrimental to the functioning of NGOs operate.

As the applicants are residents in different jurisdictions, the case of *10 Human Rights Organisations and Others v. the UK* enjoys a vast reach. In light of the above discussion, the Court's judgment on the case will bring a standard to the legitimacy of online mass surveillance programs executed in each of those countries. The verdict will not only be binding on the United Kingdom, but also (owing to its "declaratory" nature) offer guidance to Contracting States in the assessment of the compliance of their surveillance agendas and practices with the Convention. The assessment of the Court on whether the United Kingdom's mass surveillance programme, with questionable legal safeguards against arbitrary use of this power, is compatible with European human rights standards will send a clear message to similar surveillance programmes in the world, including the NSA's. The verdict on this case will expressly prompt a global consideration and a set of recommendations on the capacity of States' interception of individuals' online communications data.

One recommendation may be that for mass surveillance interferences to be legitimate, Turkey must have prior independent judicial authorization and notification to enable the affected persons to exercise their right to challenge the interception.

6.2. Collateral censorship: Ahmet Yıldırım v. Turkey

Although in the *Ahmet Yıldırım v. Turkey*[67] case, the underlying reason provided by the Turkish Court for the justification of the interference was not national security, it is important to discuss the Court's judgment as it was its first access blocking related decision. The ruling set an important precedent for the exercise of the right to freedom of expression online within the jurisdiction of the Court, and portrayed State interference by means of blocking or restricting access to the Internet as subject to strict scrutiny.

The case originated in an application by a Turkish national upon the order of the Turkish Denizli Criminal Court of First Instance to block an Internet site hosted by the Google Sites service, whose owner had been accused of insulting the memory of Atatürk, violating Internet Law No. 5651. The Telecommunications Directorate (TİB) stated that the only technical mean possible to block the "offending" site was to block all access to Google sites in general, as a result of which the applicant was unable to reach his own website. Subsequently, he lodged an application to the Court on January 2010, submitting that the blocking of all Google Sites violated his freedom of expression to receive and impart information and ideas online. He further argued that the proceeding to block access to all Google sites could not be deemed fair and impartial. The Turkish Court relied on domestic law to justify its decision, which stipulates that where a court orders the blocking of access to a specific website, the duty to implement the measure remains with the TİB. Under section 8(3) and (4) of Internet Law No. 5651, the TİB can block all access to the pages of the intermediary service provider if the content provider or hosting service provider is abroad. After reviewing the case, the Court held that the responding State of Turkey violated Article 10 of the Convention because the interference did not satisfy the foreseeability requirement under the Convention and did not afford the applicant the degree of protection to which he was entitled by the rule of law in a democratic society. The Court further found that Turkish judges had afforded too much discretion to an executive agency in dictating the measure of blocking illegal online content. The Court also commented on the lack of procedural safeguards, noting that Google Sites had neither been informed nor given an opportunity to challenge the blocking decision.

The decision of the Court as well as the non-binding concurring opinion written by judge Pinto de Albuquerque to supplement the judgment of the Court duly demonstrate the standards for the exercise of freedom of expression within the context of the Internet. According to Pinto de Albuquerque, the *Ahmet Yıldırım v. Turkey* case marks "the first time the question of freedom of expression on Web 2.0 based platforms has been put to the Court".[68]

The following section is an excerpt from that concurring opinion, which presents available references to further establish the standards of the Council of Europe on freedom of expression online. The Council of Europe's standards on freedom of expression online have been

[67] European Court of Human Rights, Ahmet Yildirim v. Turkey, No. 3111/10

[68] ibid.

introduced in various resolutions, recommendations and declarations, in addition to the Convention on Cybercrime and its Additional Protocol. Of these, the following three are especially declaratory for the present case:

- *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet;*
- *Recommendation CM/Rec(2008)6 of the Committee of Ministers to member States on measures to promote the respect for freedom of expression and information with regard to Internet filters;*
- *Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regards to search engines.*

The first recommendation suggests Contracting States to work with search engine providers to ensure that any necessary filtering or blocking is transparent to the user and that general de-indexation, which renders content inaccessible to other categories of users, should be avoided.[69] The second recommendation draws attention to the strict interpretation principle, urging that nationwide blocking or filtering of Internet content should only be permissible if it pursues one of the legitimate aims provided in Article 10 §2. The recommendation further argues that such action by the State should only be taken if the filtering concerns specific and clearly identifiable content and the decision can be reviewed by an independent and impartial regulatory body. One of the most important takeaways is the recommendation of the Committee of Ministers to avoid the general blocking of offensive of harmful content for users who are not part of the group and of illegal content for users who demonstrate a legitimate interest or need to access such content under exceptional circumstances, particularly for research purposes. The third recommendation urges States to not subject individuals to general blocking or filtering measures that go beyond than those applied to other means of content delivery. According to the concurring opinion, these documents lay down the minimum standards for the legislation on Internet blocking measures that is compatible with the Convention. Adding to these, the Judge proposes that any blocking order that is unlimited or indeterminate in duration corresponds to an unnecessary interference with the right to freedom of expression online.[70] In terms of compliance with the principle of necessity, the Judge urges for the adoption of "less draconian" measures, which translates to, for example, the adoption of a "notice and take down" policy prior to blocking order. The fact that some blocking measures may easily be evaded in the context of the Internet renders the necessity of the measure uncertain.[71] Regarding competent authorities responsible for issuing blocking order, the Judge advocates the concentration of all blocking powers in the hands of a single authority to guarantee not only the uniform application of law but also closer monitoring in practice.[72]

In a follow-up decision, the Court handled the case of *Cengiz and Others v. Turkey*. The case involved access blocking to YouTube from Turkey between 5 May 2008 and October 2010. In this case, the Court also found that the blocking of YouTube violated the right to freedom of expression. The Court held, furthermore, that Turkish authorities should have considered that blocking an entire website would block access to a large quantity of information, considerably affecting the rights of Internet users and incurring collateral damage.[73]

In line with the principle that human rights are not absolute, the blocking of online illegal content may be justified where particular circumstances apply. At the same time, blocking orders against political expressions protected by Article 10 of the Convention are unheard of in the European practice. Any interference to the right to freedom of expression by means of State surveillance can only be justified as necessary in a democratic society if and only if it avoids targeting persons or institutions not de facto responsible.

6.3. Positive obligations: Youth Initiative for Human Rights v. Serbia

The *Youth Initiative for Human Rights v. Serbia* cases primary value-added lies in its capacity to demonstrate

[69] Council of Europe, Committee of Ministers (2013): Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87>, [12], [13], [16]

[70] European Court of Human Rights, Ahmet Yildirim v. Turkey, No. 3111/10, footnote 12

[71] ibid, footnote 14

[72] ibid, footnote 15

[73] European Court of Human Rights, Cengiz and Others v. Turkey, No. 48226/10

the limits of the executive powers of States' national security services in the protection of the right to freedom of expression online.

In October 2005, the applicant non-governmental organization (NGO), Youth Initiative for Human Rights demanded the Serbian intelligence agency to provide the information on the number of individuals it subjected to electronic surveillance in 2005. In response, the intelligence agency of Serbia refused the request of the NGO on the grounds of the constitutional provision applicable to secret information. After the Information Commissioner ordered that the information requested should be disclosed pertinent to the Serbian Freedom of Information Act 2004, the intelligence agency informed the NGO that it was not in possession of the specific information requested. The NGO then lodged a complaint with the Court, under Articles 6 and 10 of the Convention, complaining of the denial of access to information held by the Serbian intelligence agency. The Court held that as the NGO pursued the legitimate aims of collecting information of public interest, conveying that information to the public and thereby contributing to public debate, the Serbian intelligence agency's refusal to provide access to public information constituted a violation of the right to freedom of expression under Article 10 of the Convention. The Court found the Agency's claim that it did not hold the information requested unpersuasive, given that it's initial claim for denying access was for reasons of secrecy. The Court further emphasized that the refusal of the intelligence agency to execute the binding order of the Information Commissioner denied domestic law and was tantamount to arbitrariness. The Court's final judgment summoned the Serbian intelligence agency to provide the NGO with the information requested.

This case is indicative of the Court's evolving standards as it embraced the right to access information even in the interest of national security. According to Strasbourg Observers, which is a blog based at the Human Rights Centre of Ghent University in Belgium to bring new judgments of the Court to attention, "[…] the case of Youth Initiative for Human Rights v. Serbia the European Court of Human Rights has recognised more explicitly than ever before the right of access to documents held by public authorities, based on Article 10 of the Convention".[74] The judgment of the Court also acknowledged the value of NGOs acting in public interest in robust terms – as a public watchdog. Furthermore, the judgment indiscriminately urged national security and intelligence agencies of Contracting States to duly respect the Convention.

In their joint concurring opinion, Judges Sajó and Vučinić highlighted particular demands of democracy in the information society as issues that the jurisprudence of the Court should address in the future. Most interestingly, they urged the Court to acknowledge the increasingly unclear discrepancy between journalists and citizens in the online world. Underlining their statement was a call to apply the principles of transparency to all citizens.[75] Another important statement set out by the Judges was that in respect of data controlled by the government, the loss of data stored by competent national authorities cannot be provided as an excuse given the complexity of modern data management tools.[76] Finally, the Judges voiced their concern over the difference between accessing information of public and personal interest, a distinction that was composed by the Court.

As to the facts of this case, the Court reassured that national authorities are under the obligation to not only refrain from arbitrary violation of the rights and freedoms in question, but also to take necessary steps to protect against the illegitimate infringement of those rights. These positive obligations require States to guarantee the compliance of their national security and intelligence agencies with the rules and principles of the Convention in the protection and exercise of freedom of expression online. As a Contracting State, Turkey should not miss any opportunity to acknowledge positive obligations. These positive obligations are particularly important for countries, such as Turkey, whose functioning of democracies is looked at with questioning stares. To comply with the mandate of the ECHR, Turkey must quintessentially secure a favorable environment for the participation in public debates.

[74] Voorhoof, Dirk (2013): Article 10 of the Convention includes the right of access to data held by an intelligence agency, <https://strasbourgobservers.com/2013/07/08/article-10-of-the-convention-includes-the-right-of-access-to-data-held-by-intelligence-agency/>

[75] European Court of Human Rights, Youth Initiative for Human Rights v. Serbia, No. 48135/06

[76] ibid.

7. Concluding Remarks

7.1. General recommendations

The ECtHR upholds its transformative role in reforming Turkey's legal system as it is binding on the Turkish Constitutional Court. European values remain an anchor for many Turks. There also continues to be popular support for the ECtHR. In a March 2018 poll conducted by Istanbul Economics Research, 47.8% of citizens supported the view that Turkey should abide by the ruling of the ECtHR on imprisoned journalists, while 35.5% were against it.[77] Yet, Turkey's compliance record is being undermined by domestic political motives. A columnist for the Hürriyet Daily News wrote in December 2017, "Turkey holds a European record that we cannot be proud of […] it is a champion in violating the European Convention on Human Rights".[78] In 2017, the ECtHR's President stated, the number of applications against Turkey increased by 276% in comparison to the year before.[79] Turkey was found to violate at least one article of the ECHR in 99 out of 116 judgments delivered by the Court in 2017. In January 2018, Turkey was criticized at the ECtHR level when a regional court refused to implement an order from Turkey's highest court to release several imprisoned journalists.[80] These furthered concerns over Turkey's judicial independence and effectiveness of its domestic remedies.

Turkey must re-orient it's ruling to the principles of the European Convention on Human Rights as interpreted by the European Court of Human Rights and try to reduce the number of cases lodged before it. The ECHR's legal sphere must represent its preferred path, just as it used to in the early 2000s when it accepted that human rights are just as valid in Turkey as in Europe. More so, Turkey should refrain from politicizing its cooperation with the ECHR. It should concede and affirm that international human rights legislations are in place to protect all members of the public. This is an integral understanding of democracy in practice, which Turkey is in need of defending.

7.2. Specific recommendations to Turkey's Internet legislation Kingdom

In its evaluation of Turkey's Internet Law, which was enacted in 2007,[81] the Representative of the Organization for Security and Co-operation in Europe (OSCE) argued that the banning of websites, such as YouTube and Google Sites has very strong repercussions on political expression. Turkey's approach to Internet publications and content, with regular blocking orders enacted by national courts and the Presidency of Telecommunication and Communication (abolished in 2016 with powers transferred to the Information and Communication Technologies Authority (BTK)) was deemed essentially problematic because it blocks access to not only allegedly illegal content but also to legal content and information. As a result of its evaluation, OSCE urgently called on the Turkish government to bring its Internet Law in line with international standards, which should otherwise be abolished.[82] In a similar effort, in 2011, the Commissioner for Human Rights of the Council of Europe recommended Turkey to review its Internet Law against the standards accepted in the European case-law. One of the reasons for such recommendation was that the grounds for allowing access blocking to websites were broadly interpreted.[83]

This paper recommends Turkey to bring its Internet governance closer to the European practice. To this end, Turkey is firstly advised to remain aware of and receptive to the ECHR's evolving standards and regulations in cyberspace. For Turkey's Internet legislation to meet the

[77] Istanbul Economics Research (March 2018): Turkey Monitor [unpublished]

[78] Ergin, Sedat (2017): Turkey is the champion of rights violations at the ECHR, <http://www.hurriyetdailynews.com/opinion/sedat-ergin/turkey-is-the-champion-of-rights-violations-at-the-echr-124411>

[79] DW (2017): More than 5,000 cases filed against Turkey over post-coup purge, says ECHR, <http://www.dw.com/en/more-than-5000-cases-filed-against-turkey-over-post-coup-purge-says-echr/a-37294226>

[80] Delegation of the European Union to the Council of Europe (2018): EUDEL statement on the implementation of the decision of the Constitutional Court of Turkey, < https://eeas.europa.eu/delegations/council-europe/39162/eudel-statement-implementation-decision-constitutional-court-turkey_en>

[81] For a detailed evaluation of Turkey's Internet Law please see Ergun, D (2018): National Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy.

[82] Organization for Security and Co-operation in Europe (2010): OSCE Representation on Freedom of the Media Report on the Turkish Internet Law, <https://www.osce.org/fom/41091>

[83] CommDH (2011), Report by Thomas Hammerberg Commissioner for Human Rights of the Council of Europe following his visit to Turkey from 27 to 29 April 2011, <http://www.refworld.org/docid/4ecbc1952.html>

appropriate standards of Europe, this paper formulates several main recommendations in line with the suggestions of the Venice Commission.[84]

Turkey's Internet Law should include a provision on "strong public interest". As provided in previous chapters, the ECHR upholds that there is a strong public interest in protecting individual rights and freedoms. ECHR's principle essentially argues that the society benefits as a whole when individual rights and freedoms are duly protected. As noted by the Venice Commission Turkey is recommended to include a "strong public interest" clause in its Internet Law. Given that the ECHR affords the press the right to impart and receive information on matters of public interest, the recognition of "public interest" within the Turkish human rights regime would better protect journalists and publishers. It would also consolidate Turkey's understanding of the press as a political watchdog, an idea that is strongly advocated by the ECHR.

Turkey's Internet Law should provide a list of less intrusive measures. When assessing the decision of national courts, the ECtHR always considers the severity and nature of the restriction imposed. To ensure that public debate is not hindered, the sanction must only be the least intrusive measure available. In the context of Turkey's Internet Law, the only measure available is access blocking or removal of content, which the European regime deems the most severe measure possible on the Internet. Turkey is strongly recommended to include in its Internet Law a list of less intrusive measures, including obligation for explanation, correction or content renewal. This would provide Turkish judges with sufficient room to assess and execute the least intrusive measure available in satisfying the legitimate aim pursued by the restriction, and thus bring Turkey's Internet legislation more in conformity with European standards.

Turkey's Internet Law should include a provision on democratic necessity and proportionality. According to the European practice, any blocking or removal measure on the Internet should fulfill the duty of democratic necessity. To this end, the competent authority in Turkey should internalize the case-law of the European Court of Human Rights, particularly on cases concerning the freedom of political speech. One way to ensure this is to amend Turkey's Internet Law to include a specific provision to guarantee that the restriction is necessary in a democratic society and is proportionate to the legitimate aim pursued.

Turkey's Internet Law should provide sufficient notification procedures. The European practice urges national legislations to provide related parties with notifications concerning the procedures of access blocking or removal of content. To this end, Turkey is recommended to notify all affected individuals by providing information about the blocking/removal measure, its justification and existing remedies.

Turkish courts should prioritize cases concerning access blocking. The Convention recognizes the fundamental role played by the Internet in granting the public access to information. Turkey is recommended to prioritize in practice those cases regarding access blocking on the Internet. Additionally, in line with the Venice Commission's recommendation,[85] Turkey is advised to constantly apply a "practice of urgent procedure" to cases concerning online rights and freedoms and to provide a publicly available registry of pending cases. Furthermore, Turkish authorities are recommended to publish official numbers of blocked websites or URLs.

To satisfy these recommendations, Turkey should periodically assess its level of respect and protection for the exercise of human rights and freedoms on the Internet, including evaluations on governance accountability and transparency mechanisms. As a State party to the Convention, Turkey must never de-prioritize its positive obligations to enable a favorable environment for Internet freedoms.

[84] Venice Commission (2016): Opinion on Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by means of such Publication ("The Internet Law"), <http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e>

[85] ibid.

Centre for Economics and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2018/3

April 2018

Online freedoms and the European Court of Human Rights: a path forward for Turkey?

Yeşil Deniz | Research Assistant, EDAM